2004年度　修士論文

個人向けサービスにおける
プライバシ制御

提出日：２００５年２月２日

指導：中島達夫　教授

早稲田大学大学院　理工学研究科
情報ネットワーク専攻
学籍番号：3603U077-8
正寺　朋子

目 次

図 目 次

表 目 次

概 要

個人情報やコンテキスト情報を利用した個人向けサービスを提供するようなアプリケーションの開発が進む中，一般消費者からのプライバシ保護への興味が高くなってきている．しかし，プライバシ保護の問題というのは，社会学的観点や，心理学的観点などさまざまな観点から検討される必要があるので，技術者が技術的対策のみを考慮して対策を検討することには限界があることが問題として考えられる．そこで，実際にプライバシ保護に関する問題として九つの論点を用意し，それぞれの論点に関して，技術的・非技術的の両視点から問題の考察をおこなうことで，プライバシ保護を実現するためのシステムを評価するフレームワークの構築をおこなう．その上で，実際に実装したシステムを評価し，プライバシ保護を実現するためのシステムに不足する部分があるかどうか検証する．

Abstract

As the techniques for the applications of the personalized services are being developed, the user's interest of privacy-protection becomes higher. However, the problems for the privacy-protection can not be solved, if it is only concerned from the systematic point of view, but also needed to be concerned from some non-systematic point of view, like, socially, legally, etc.

Therefore, I prepared 9 points of contention as the problems to concern about privacy-protection. Then, by considering these 9 contentions, I propose the framework which evaluate the system which implement to protect the privacy.

In addition to that, I evaluate my own system, called *Panates* (Privacy protEctioN Architecture for contexTaware EnvironmentS) which makes it possible, the user control own personal information, and the transaction of personal information be seamless, based on that framework, and examine what is missing this *Penates* to be the perfect system to protect privacy.

第1章　序論

本章では，本研究をおこなうことになった目的について論じるとともに，本研究をおこなう上で参考にした法的規制についての概要を紹介する．さらに，本研究において利用した言葉で一般的解釈が複数存在する単語の定義付けをおこなう．

1.1　背景

近年，ユーザの名前・年齢・性別といった個人情報や，ユーザが今いる環境の情報を表すコンテキスト情報などを利用することで，そのユーザに適したサービスを提供する個人向けサービスが増加している．それに伴って，一般消費者が，自分の個人情報を自分で管理する必要性が高まってきた．また，このような環境の中においては，できるだけ自然にそのユーザに適したサービスを提供することが特徴としてあげられるため，円滑な情報の取り扱いが必要とされる．

そのような背景の中，プライバシの保護を実現させるために様々な研究がおこなわれている．しかし，現状として，完全にプライバシを保護できると保証できるようなしすてむが存在していないのは事実である．そこで，既存の研究を調査したところ、技術的対策 [2] と非技術的対策 [4] が完全に別々の研究としてとおこなわれているため，それぞれの対策の間に溝が生じてしまっていることがわかった．

1.1.1　個人向けサービス

まず始めに，個人向けサービスとはどのようなサービスを指しているかについて説明する．背景で記述したように個人向けサービスとは，ユーザの名前や年齢・性別といった個人情報や，そのユーザが今いる環境の情報等を表すコンテキスト情報を利用することで，その人の趣味嗜好・現在の状況に合わせたサービスを提供するアプリケーションである．

このようなサービスでは，個人情報を提供することによる情報漏えいの危険性とサービスのクオリティ向上という二つの要素はトレードオフ[1]の関係にあるといえる．従って，サービスのクオリティ向上のみを考慮して無作為に個人情報を提供することは，自分の情報を漏えいさせる危険性を高めることになり，非常に危険な状況に陥りかねない．そこで，このような状況下では，一般消費者が自分で自分の個人情報をきちんと管理しなければならないのである．

[1] トレードオフ：ある関連する二つの事象に対して，一方を犠牲にすることでもう一方の利益が上がるといったように，複数の条件が同時に満たすことがないような関係のこと

1.1.2 個人情報とプライバシ情報

次に，個人向けサービスにおいて必要とされる個人情報とは，主にどのような情報を指すのかについて説明する．一般的に個人情報と呼ばれる情報には,「プライバシ情報」と「個人情報」の二種類がある．本論文におけるそれぞれの定義は以下の通りである．

プライバシ情報

プライバシ情報とは，ユーザに関わる全ての情報であり，ここでは主に，位置情報等その情報だけでは個人を特定することはできない動的情報をさす．ユーザを取り囲む空間における情報は，ユーザにとっては自分の情報を表す情報であるが，その情報のみが外部に流出したところで個人を特定することはできない情報である．

この情報が何らかの情報と結びついて個人を特定できる状態になったらそれは個人情報と呼ぶことにする．

個人情報

従って個人情報とは，個人を特定することが可能な情報であるとする．主に住所氏名などの静的情報は個人情報になり易い．また，先ほど定義した動的情報等のプライバシ情報も，静的情報と結びついて時点で，個人情報という個人を特定できる情報になる．

このように，個人が特定されてしまうような情報を取り扱う際には，十分な注意が必要であり，この注意が十分でないと，個人情報の漏洩の問題が発生したり，プライバシの侵害であったりという問題が発生するため，便利なサービスを作ったところで，それをユーザが受け入れないといった問題が発生する恐れがある．

1.2 法的背景

プライバシの保護を実現する上で，さまざまな法案が規制されている．実際に，プライバシを保護するためには，無作為に情報を外部に提供しないようにすると共に，提供した情報が十分なセキュリティ対策の基で管理される必要がある．直接的にこれらを規定しているのが，プライバシ保護法と個人情報保護法である．以下にそれぞれの概要を記す．

1.2.1 プライバシ保護法と個人情報保護法

そもそも，プライバシ権とは何なのかという定義が最近不明確になってきている．文献 [7] において，牧野氏は「プライバシとは場所的・空間的領域概念であり，茫然たる多数の権利を包摂する最も価値の高い部分である．プライバシ権とは，こうした空間に無断で介入することを拒否し，自らの情報を提供することの可否を決定する権利（自己決定権）を包摂するものである.」と定義している．また,「個人情報保護とは，管理されている情報の管理，利用，処分に関する基本的ルール（ガイドライン）であり，個人情報保護法とは，情報管理者規制・規律法である.」と定義している．従って，

「プライバシ保護法と個人情報保護法との二つの法律が必要であり，両者を混同する議論は，プライバシの未来を暗くする危険がある」のである．

では，個人情報の取り扱いについてはどのような点に考慮する必要があるのだろうか．上記に記したようにこれについては，個人情報保護法に定められた規定がある．この法案は近年の，デバイスの小型化やインターネットの普及に応じて改正が考慮され，規定し直された物であるが，この法案で完全に個人情報を保護できているかというと，今後の個人情報を利用した上でのサービスにおいては，考慮しきれていない部分がまだ残っている．

1.2.2 個人情報の保護とは

個人情報の保護とは，個人情報を外部に出さないようにすることではなく，提供する個人情報に関して，自分がどのように管理・把握するのかということであると定義する．

技術的に完璧に個人情報を保護するということは，不可能だと考えられる．そこで，法案が必要とされるわけだが，実際には，法案というのは，侵されることが多くあり，それを罰則だけで保護するには無理があるので，何をどの程度保証することが一般消費者の利用を促すことになるのかという点について考慮する必要がある．

そこで，何をどうすることが，消費者に新しいサービスの利用を促すことになるのかについて検討してみた．一番問題となっているのは，本人の知らないうちに大量の個人情報がコンピュータ等の情報機器に蓄積される機会が増加しているということである．このような環境では，本人の予想しなかった目的で個人情報が利用されるという事態が発生し，こういった事態が発生すると，消費者の立場としては，個人情報が勝手に取り扱われてしまうような新しいサービスには利用の抵抗感が生まれてしまうのではないかと考える．

結果的に，現在想定しているような個人向けサービスを提供するようなアプリケーションが増加するような環境における個人情報の保護とは，個人情報を利用することによって，サービスをより自分に適した物にすることを前提として考慮されるべき問題なので，消費者が個人情報を安心して提供してくれるような環境を作り出すことによって，個人情報をある特定の目的で提供しても，それ以外の目的では利用されないということを保証して，その約束が破られないことを保護することであると考えられる．

個人情報保護法案

個人情報保護法は，近年になって考えられた完全に新しい法案というわけではない．個人情報を保護する目的の法案は以前からあったが，インターネットの普及等に伴い，以前の法案では保護しきれなくなってきたため，新たに再検討されたのである．以前の法案においては，個人情報を取り扱う者としては，公的部門の国の行政機関であったり，地方公共団体であったりといったような団体が対象とされていたが，現在のような環境においては，民間部門が取り扱うことが多発したため，公的部門の規制の再検討と共に，さらに，民間部門における規定を追加したのである．個人情報保護法の詳細に関しては，付録 C に記載した．

法が整備された背景

プライバシの権利とは，当初米国で一部マスメディアとの関係で「一人で放っておいてもらう権利」として誕生した物である．現在は，情報化社会の進展を受けて日本においても検討されるようになったが，現在検討されているプライバシの権利とは，「自己情報をコントロールする権利」としての見解が提唱されており，このような見解が広まるにつれて欧州諸国でもこの法制が普及してきたといえる．前者の見解は，マスメディアプライバシと呼ばれているのに対し，後者はコンピュータプライバシと呼ばれている．このような流れを受けて，１９８０年にOECD(経済協力開発機構) が「プライバシ保護と個人データの流通についてのガイドラインに関する理事会勧告」を公表した．このように，世界的機構が勧告を公表するには次のようなわけがある．

コンピュータプライバシを検討する際に気をつけるべきことは，ここで取り扱われている個人情報は，コンピュータに貯蓄されている情報であり，このコンピュータがインターネットでつながれていることによって，どこにでも簡単に漏洩する可能性があるということである．インターネットの世界は，国境のない世界なので，いくら自国で厳しい法案を発令したところで，個人情報が他国を通じて自国に入ってきた際，その他国においては自国で違反なことが認められていては罰することができないといったような問題が生じるのである．

日本においては，OECD の勧告を受けて，これに対応するための行政機関保有個人情報保護法が制定されたが，１９９５年に EU が「個人データ保護指令」を採択し，この指令においては，個人データを EU 域外に輸出するための条件として，民間部門を対象とする物も含めて，EU 域内並みの個人情報保護法制の確立を求められたので，日本においても制度的な対応が求められた．この際，日本には，民間部門を対象とする個人情報保護法制が存在しなかったので，新たな法設備が必要とされたのである．

これに加え，同時期にインターネットの普及が高まり，個人情報の漏洩や，セキュリティが不十分なことからおこるウィルスの感染，それに伴う悪影響による問題が急激に増加したことを受けて，オンラインプライバシという概念が強く意識される物となり，このような中で，住民基本台帳法改正の際に，個人情報保護法制の設備が必要不可欠となり，立法化に至った．

目的と概要

既存の法案が規定しているのは，個人情報を違法に取り扱われた本人（個人情報によって識別される特定の個人）に対する損害賠償を中心とする責任であり，新しくできた法案が規定しているのは，主として，監督官庁から行政処分を受けるという内容の責任である．また,「個人の権利利益」を保護する際に,「個人情報の有用性に配慮」すべきであることも明記されている．これは，前にも述べたように，個人情報を示す本人側にとっても，有用性が存在していることが必要とされているということである．

これらを基本事項とし，個人情報の適切な取り扱いに関し定められている詳細は最後に記述する．

1.3　研究目的

以上のことを考慮した上で，本研究の目的は，プライバシ保護を実現するシステムを評価するためのフレームワークを提案し，実際にプライバシを保護するために実装

したシステムを評価することである．フレームワークの提案は，個人情報を取り扱いに当たって注意しなければならない要素を，自分が今までおこなってきた研究で得た知識を基に九つに分類し，それぞれを論点とし，技術的のみならずさまざまな視点から考察した結果をまとめたものである．

実際に評価をおこなう上で利用したシステムは，ユーザに自分の個人情報を自己管理させた上で，円滑な情報の取り扱いを可能にするために実装したシステムである．このシステムを基に，プライバシの保護を実現するための基盤を提供するにはどのような要件に関して検討する必要があるのかということを把握することを最終目的とする．

1.4 論文の構成

本論文では，個人向けサービスにおけるプライバシ制御について考察するために，大きく九つ論点を用意している．そこで，第２章においてそれぞれの論点の詳細な説明を論じる．第３章では，第２章で説明した論点を考察した結果導きだされた要件について論じ，第４章で関連研究を紹介する．そして，第５章で将来課題を挙げて，第６章で結論を論じ締めくくる．当論文で紹介したシステムの詳細や，利用した法律を自分なりにまとめた概要に関しては，最後に付録として添付する．

第2章　個人情報利用に伴う九つの論点

本章では，個人向けサービスが提供されるような環境において，プライバシの保護を実現するシステムを構築する際，考慮すべき個人情報の取り扱いについての注意事項として九つの論点を紹介する．これらの論点は，今まで自分が個人情報の取り扱いを研究してきた中で得た知識を基に検討すべきだと判断した項目を九つに選別したものである．

序論で記したように，プライバシという言葉には様々な解釈があり，混乱しやすいので，本研究におけるプライバシの定義を定めた．本研究におけるプライバシとは，私的領域を自分でコントロールする権利であると定義する．従って，プライバシを保護するとは私的領域を自分でコントロールする権利を保護する事になり，私的領域とは何かという点が問題になる．私的領域とは，自分が存在する領域であり，自分の存在を表す全ての要素がその領域内に存在するのである．以上を考慮すると，プライバシの保護とは，自分自身を示す個人情報を始め，自分が存在する空間の情報であるコンテキスト情報等全ての情報を自分でコントロールする権利を保護することになる．

ここで，これらの九つの論点に関する考察をおこなう上で，図 2.1 のように大きく四つのグループに分けた．

- 1.技術的対策が必要とされる論点
  - 1-1.個人情報の自己管理
  - 1-2.評判システム
- 2. 非技術的対策が必要とされる論点
  - 2-1.グローバルな法的規制
  - 2-2.セキュリティ
- 3.非技術的対策をバックアップするための論点
  - 3-1.個人情報提供の判断基準
  - 3-2.人間とサービスの関係
  - 3-3. 他人／インターネット／サービスに対する信頼性
- 4.今後新たな問題として考えられるであろう論点
  - 4-1.個人情報の抽象化
  - 4-2.自動的に取得されてしまう個人情報

図 2.1: 九つの論点

この分け方は，それぞれの論点に関してさまざまな視野からの検討をおこなわなければならないという前提のもと，現状で提供されている解決策だけでは足りない問題を解決するためにどのような視野からの検討が必要とされるかという点で分けたものである．グループ１は，法的規制としては整っているものの，実際にその法を生かした技術的対策が不足していると考えられる論点．グループ２は，技術的な発達に伴っていろいろなことが可能になっている中，法的規制がきちんと整っていないために技

術の進歩を生かしきれないという危機があるため，きちんとした規制が必要とされている論点．グループ３は，グループ１・２で利用されている非技術的対策をバックアップするための概念を定義するための論点で，法的規定のみならず，社会学的また心理学的観点から検討する必要があり，最後に，グループ４は，今後新たな問題として考えられるであろう論点で，技術的・非技術的の両視点からの対策が必要とされている．

プライバシを実現するためのシステムを構築する際には，これら全ての論点に関して検討する必要がある．そこで，検討すべき論点の考察をまとめ，最後に論点１－１で紹介するシステムを完全なプライバシ保護システムとするための要件をまとめる．

2.1 論点１－１：個人情報の自己管理

１章の前提をもとに考えると，今後，一般消費者は自分で自分の個人情報を管理しなくてはならない．しかし，個人情報の自己管理といっても，データの管理なので，目に見えるものを管理するのと異なり難しいものである．ここでいう個人情報の自己管理とは，データの管理がメインなのではなく，ユーザが自分の個人情報がどこでどのように利用されているかということをきちんと把握することを目的とする．

この論点における問題は，次の通りである．

- 個人情報の利用用途を如何に把握するかが明確ではない
- 要求される度自分で個人情報を提供するのは円滑な取引の妨げになる
- 自己管理のための判断基準がない

実際，現状では，個人情報の自己管理を実現するための非技術的解決策として，いくつかの法的規制が用いられている．序論で紹介した個人情報保護法等がそれにあたり，個人情報を収集する事業者は，要求する情報に関して要求者にその利用用途等の情報を明示的に示さなければならないことになっている．また，一度収集した情報の管理についても，十分なセキュリティ対策を用いて管理する責任があることを規定している．これに関しては，企業がどのように対処すべきかというガイドラインも検討されている [16].

しかし，これらの対策では，誰がどんな責任を持っているかということを明確にしているだけで，その責任を全うするためにどうしたらいいかということは定められていない．そこで，この問題に対する技術的解決として，ユーザに個人情報の利用用途に関する情報を半強制的に提供し，且つ，円滑な情報の取り扱いを可能とするためのシステムが必要とされる．これによって，個人情報の自己管理における問題を技術的に解決できると考えた．

そのため，次のようなシステムの構築をおこなった．

2.1.1 ポリシ・プリファレンスマッチングシステム (Penates)

ここでは，筆者が実装したポリシ･プリファレンスマッチングシステム (以下 Penates[1]) [3] の説明をおこなう．本システムは，次のような考えのもと設計された．

消費者が個人情報を要求された際，なぜ戸惑うかを考えると，まず第一に，自分の個人情報がどのように利用されるかわからないであるとか，自分の個人情報が漏洩することへの恐怖感等が考えられる．実際には，前述したように，個人情報保護法でこの問題が解決されるよう定義してあるが，実際どのように利用方法等を知ることができるのだろうか．これを検討する際に，もう一つ考慮しなければならない点がある．それは，如何に自然にそれを把握することができるかということである．自分の個人情報が何のために誰に利用されるのかを知ることは，自己管理をする上で必要不可欠なことだが，そのための莫大な手間がかかるのであっては，元々のサービス提供の主旨を外れてしまうのである．デバイスの小型化やインターネットの普及による新サービス提供の主旨の一つとしてあげられるのが，個人情報や趣味嗜好を取り入れて自然にそのユーザに適合したサービスを提供するということである．そのため，いくら自己管理のためといえども，サービスを受ける前に莫大なる資料を読まないといけなかっ

[1] Penates：Privacy protEctioN Architecture for contexTaware EnvironmentS の略

たり，面倒な手続きが必要だったりでは本末転倒なのである．そこで，如何に円滑に取り扱いをおこなうかということを考慮した上で Penates を構築した．

まず，サービス提供側がポリシファイルと呼ばれる，個人情報の利用目的や，利用方法等を詳細に記述したファイルを用意し，ユーザはプリファレンスファイルと呼ばれる自分がどの個人情報をどのような利用目的で利用されることを許可するか等について定義したファイルを用意する．制御の流れは図 2.2 に示す通りで，ユーザがあるサービスの提供範囲内に入ると，ユーザの持っているデバイスが検知され，ポリシファイルとプリファレンスファイルが比較を始める．そこで，提供が許可されている個人情報の利用用途がポリシファイルで要求されているその情報の利用用途が一致すると認められたら，その情報を自動で提供するといったものである．

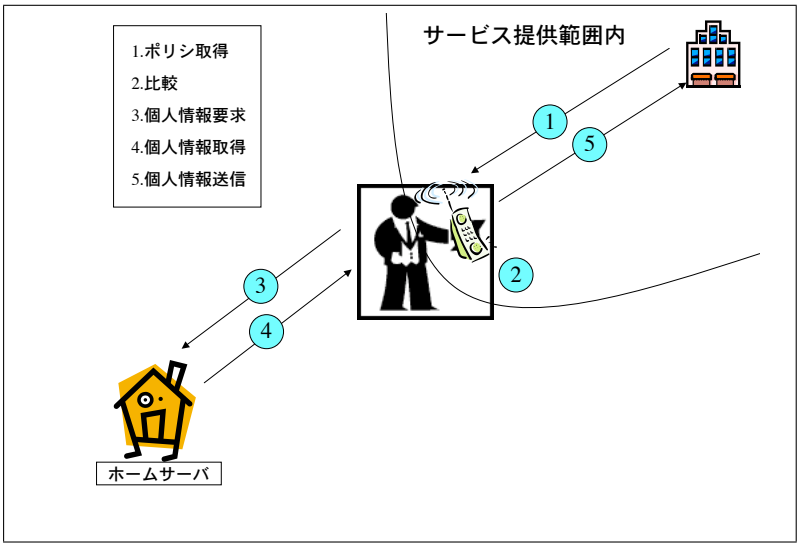

図 2.2: Penates

詳細は付録 A に記述する．

このようなシステムの構築に伴い，ユーザは個人情報を必要とするような多種多様なサービスの提供を受けるためにいちいちその個人情報を提供するための手はずを自ら意識しておこなう必要はなくなる．また，個人情報の利用方法に関しては，自分が自動提供を許可してるもの以外は，利用目的等を通知されてから自分で提供を判断できることから，ユーザ自らが自分の個人情報を自己管理できるという状態を提供することができるのではないかと考えた．

しかし，本システムを設計する際には，技術的視野からのみ検討したため，実際に稼働させることを考えると，いくつかの問題が生じることがわかったので，それについて以下に詳細を記す．

2.1.2 統合的な視野からの対策

問題とは，この Penates をその目的通りに稼働させるには，いくつかの保証されるべき前提条件が必要となっているという点である．これらの前提は，システム設計をおこなう上で，システムで補いきれない部分に対して，その部分は非技術的解決策を提案している人達に任せようということで，具体的にどんな対策が必要とされるかを検討することなく済ませてしまったことによって発生したと考えられる．

従って，既存の非技術的解決策で保証されている部分と，Penates で保証されている部分を統合的に考えて，全体として後何が保証されなければならないのかを検討した．

現状の前提条件

このシステムでマッチングをおこなってから個人情報の提供をおこなうことで，ユーザが自分の個人情報を自分で制御するための助けになると考えられるが，そのためには，次の前提が成立する必要がある．

1. サービス提供側はポリシファイルに定義されている通りに個人情報を取り扱う
2. 両ファイルの比較は適切におこなわれる
3. 一度収集された個人情報は十分なセキュリティの基に管理される
4. 初期段階のプリファレンスシステム作成方法は，一般ユーザにも作成しやすい

実際に，いくつかの前提に対しては，非技術的対策が施されている．例えば，前提１・２・３に対しては法的に規制されている．しかし，法的に規制されていれば問題がないというわけではない．通常，法的に規制されているということが保証になるのだが，一般ユーザに取っては法的に規制があるというだけでは納得しにくいものである．悪用されたり，漏洩したりという点に懸念を持って躊躇しているユーザに対し，法的に規制されているからという理由では納得させられない．

では，補いきれない部分に関してどのように対処すべきかということが問題になるわけだが，前提１・２の要素とは，個人情報を渡す相手として信頼のおける相手かどうかということを判断するために必要とされる要素だが，この要素に関しては，数値的に提供できる基準が存在しないので，論点３－３にて概念を理解し，その上で判断基準として，他の判断基準を提供するということで解決としたい．この判断基準という概念については，論点３－１で論じる．また，判断基準という論点における解決策の一つとして，評判情報が考えられ，それを提供する評判システムが考えられる．これに関しては，技術的解決策が必要とされている論点なので，次の論点１－２で論じる．さらに，前提３のセキュリティ対策に関しては，論点２－２にて詳細を論じる．ここでは，前提４について論じることとする．

個人情報管理のための初期導入作業

Penates で一番の問題となる箇所は，初期導入作業についてである．本システムは，一般消費者がサービスを利用する上での取引を円滑におこなえるようにするためのシステムなので，利用者である消費者にとって難しい手順があったり，理解しにくいようでは意味がなくなってしまう．

実際に，プリファレンスファイルをうまく用意すれば，煩わしい手間を省いて自ら自然に個人情報の自己管理をおこなうことが可能だが，そのプリファレンスファイルをうまく作成するという作業自体が一般消費者にとって，とても難しいことになると考えられる．

プリファレンスファイルは，XML ファイルで作成されており，このファイルへは，例えば，各個人情報項目毎に，どの程度の利用を許可するかチェックボックスのような

ものでチェックすることにより自動的に XML 形式に変換することは可能となる．しかし問題は，ユビキタスコンピューティング環境下において，どんな個人情報がどのような利用目的で利用される可能性があるのかということを全て把握するのは非常に困難であるという点である．また，個人情報の量は詳細に切り分けると無限大にあり，それら全てについて全ての利用される可能性に関して考えるには膨大な時間がかかり，それを考えるくらいなら，利用される毎に聞かれたほうが楽だという考えが生じてしまうのである．

そこで，このシステム導入のために，まず考えるべきことは，

- プリファレンスファイル初期導入方法
- 使い易いユーザインタフェース

の２点である．

システム導入のための初期段階としてどのように初期設定をおこなうことが消費者にとって一番有効的なのかということに関しては，まだまだ検討が必要である．また，現段階では，頻繁に要求されると考えられる ”住所・氏名・年齢・電話番号 ”等のいくるかの主要個人情報に関しては，初期設定段階で，できるだけ詳細に定義しておき，サービス毎に要求されるかどうかが異なる情報に関しては，その都度直接設定することがいいのではないかと考える．さらに，個人情報を詳細に定義しておくということに関しては，論点４－１で個人情報の抽象化の問題として論じる．

さらに，サービス毎にプリファレンスを持つことで，再度同じサービスを受ける際に，同じ設定をおこなわなくてすむようにできる．先に論じたように，全ての可能性を前もって定義しておくことは不可能なので，最良のシステムを用意することができたとしても，ユーザに多少の手間がかかることになるが，個人情報を自己管理することがプライバシ保護のためにどれほど重要かということを各個人がきちんと認識することも必要なことの一つである．従って，多少の手間がかかってでも対処しなくてはならないことがあるということを認識することも必要なのである．

サービスを提供するという意味では，できるだけ自然にことを運べるような環境を提供したいと考えるが，そのような環境が構築されるためには，まずユーザ一人一人が個人情報管理の重要さを把握し，プライバシ保護をすることの重要性を理解することが必要である．

2.1.3 論点１－１まとめ

個人情報の自己管理における問題点を抽出し，それの解決策として，既存の非記述的対策を基に技術的対策としてシステムを組み込んで更なる問題点を抽出した．またその中で，技術的対策と非技術的対策を別々の対策として考えることは，両対策の間に溝を生むことになり，どちらの対策にも解決策が提案されていない問題を残してしまうことになることを挙げ，常にさまざまな視点から検証することの重要性を示した．

個人情報とは形あるものと異なり，データなので，普通に考えて一般消費者がデータベースを作成してそれを管理し，必要なときに取り出し利用するというのは考えにくい．そこで，とりあえずユーザが自分の個人情報がどのように利用されるかということに関してきちんと把握し，納得した上で個人情報を提供するといったことが可能になるよう Penates を実装した．

本システムが必要とされるような環境が実際に構築されるようになるまでに，前述した問題や，次以降に論じる問題について解決策が見いだされることが必要不可欠である．また，前節最後で論じたように，自己管理をおこなうには，個人個人がその必要性を十分に理解し，きちんとした対処をおこなわないことの危険性を理解する必要があると考える．これに関しては，政府機関がそれ相応な対応をすることで国民に理解させる必要があるのではないかとも考える．それは，こういった環境の延長上に電子政府[2]という新しい政府のあり方が関連してくるからである．電子政府に関しては，関連研究において，GBDe が電子政府構築の際のガイドライン [10] を提言しているのを記載した．

また，本論点において，検討すべき問題を解決する上で他の論点を参照するよう指摘したが，実際には本論点で挙げた項目のみならず，全ての論点における考察を検討することで，Penates をプライバシを実現するためのシステムとして完成させることができるのである．従って，Penates は本論点における問題の技術的解決策として提案したシステムだが，各論点の考察をまとめた最後に Penates を完成させるための要件についてのまとめを考察する．

[2]電子政府：政府の所有する国民の情報をネットワーク上で管理して，さまざまな手続きが円滑におこなわれるようになるために考えられている新しい政府の形

2.2　論点１－２：評判システム

評判システムとは，一見プライバシの保護という要素とは関係ない話のように思われるが，論点１－１で論じたように，プライバシの保護を実現するためには，個人情報を自己管理する必要があり，個人情報を自己管理するための判断基準（詳細は論点３－１）の一つとして，評判という要素が挙げられるのである．

評判システムとはある特定の事項に関して人々がどのように感じているか，思っているかといったような情報をまとめて消費者に提供するようなシステムのことである．このシステムの有効性を検証するために，まず評判情報というものが消費者に与える影響について調べた．

2.2.1　評判が消費者に与える影響について

評判が一般消費者に与える影響は，”インターネットでの評判と広告の実証的研究 [5] ”によって証明されている．この研究では，情報の信頼性判断基準としての評判の形成過程とその消費行動に与える影響について研究をおこなっている．以下に概要をまとめておく．

インターネット空間における信頼

口コミ等の対面コミュニケーションに比べて相手を直接コントロールする方法が小さくなり，信頼が裏切られる可能性が大きくなるのがインターネット空間などにおける場合である．多種多様な人々から情報が得られるという意味で，信頼が報われたときの利益は大きくなるが，匿名の人が相手なので如何に信頼を得るかが問題となってくる．

一般的に，関係に束縛されない人間性を判断することに適にしていて不特定多数の他人を信頼する高信頼者と，人間関係の性質を判断する能力に優れていて，他人との関係についての地図をうまく立ち回れる低信頼者がいると考えられるが，インターネット空間で利益を受けるのに有利であるのは高信頼者だと考えられる．しかし，必要な情報が提供されなければ，他者を信頼するという行動はリスクテイキングではなくただのギャンブルになってしまう．そこで，信頼性をどのように判断しているのかということが重要になってくる．

信頼性の判断

ネット環境における情報の流通はその情報を信頼するところから始まる．しかし全ての情報が信頼のおける情報というわけではなく，情報を収集する者としてはどの情報に信憑性があり，どの情報にはないのかという点について十分考慮する必要がある．

文献 [5] において,「一般に，多くの人がある対象に対して同じ内容の情報（評判）を書き込んでいれば，多数派のヒューリスティック，すなわち「皆が信頼しているから」という考えが働き，その情報の信頼性や妥当性が高くみなされることがある．また，自分の既存の知識や体験に基づく信頼性の判断というのもよく取られる手段の一つであると考えられる．この他にも，自分の信頼している人の情報だからという対人関係に基づく信頼性の判断や，社会的に信頼できている物と同じ情報であると言ったような制度に基づく信頼性の判断，相手の過去の実績に基づいた信頼性の判断，そし

て他のメディアを使った情報の確認をおこなうといったような物まである.」と定義されている.

では，ネット空間における信頼もこれらの定義に基づくような信頼なのであろうか.ここに定義したような対人関係や自分の経験等を軸に考えると，多種多様な情報を網羅しているネットの特徴を生かせないことになるのではないだろうか．そこで，信頼性を判断するための評判という概念が生まれるのである.

信頼性を判断するための評判

評判とは，他者によっておこなわれる，”ある人について記述される特徴や属性のこと ”である．これは，過去の行動が将来の行動を予測するという仮説の基に成立しており，評判を立てられた相手の人間性を判断するための情報としての機能を果たすだけでなく，評判を立てられる人の行動をコントロールする役割を果たしている．本研究の場合，評判の対象は人ではなくサービスだが，この場合でも同様なことが言えると考えている.

サービスを評価するための評判という情報は，ユーザにとってそのサービスを利用するか否かの判断基準になるだけではなく，評判が立つということ自体が，サービス提供側のクオリティ向上を促し，セキュリティ強化を促すことになるのである.

Kollock.P 氏は，信頼性を判断するための評価は次のような要因によって促されていると定義している．第一に，自分が情報を提供することと引き換えに有効な情報や手助けを得られるであろうことを期待して，価値ある情報を集団に提供するという互恵性．第二に，発言によるオンラインコミュニティへの貢献によって，自分の評判を高めたいという自己顕示欲．第三に，自分が環境に何らかの効果を及ぼしたい，または自分が役立つ人間だという自己イメージを形成したいという自己満足．第四に，愛着や関与からなるオンラインコミュニティの一員だいう連帯感．この意見は，他の文献からも同様なリサーチ結果が生まれていることから信憑性は高いと考えられる.

2.2.2　評判に求められる情報

では，一般消費者が評判を求めるときはどんなときだろうか？個人情報を出すか否か迷ったときというよりはそもそもサービスのクオリティを知りたいときかもしれない．大きく分けると，評判としてほしい情報には二つのタイプがあるのではないだろうか.

一つ目は，実際にサービスを受けた人がどの程度の情報を提供してどの程度のクオリティのサービスを受けた上でどんな評価を下したかという情報である．これは，アプリケーションに特化した評判システムで，サービスのクオリティごとにその評価情報が検出される．既存のシステムとしては，インターネットオークション市場で評判システムとして稼働しているものが同様の働きをしている.

二つ目は，口コミのような情報である．このような情報では，実際にそのサービスを受けた人からの評価かどうかは保証されないが，一般的にどのような印象を持たれているかと言ったような情報が分かる．これは，ネット上の blog 等に個人が載せた情報や，誰もが書き込める掲示板等の情報をクローリングしてサイトの内容解析することで評判として提供される.

次節に，以上の 2 種類の情報を提供する評判システムの詳細について示す.

2.3　論点１－２－１：アプリケーションに特化した評判システム

2.3.1　既存の評判システム

まず始めに，既存の評価システムにはどのような機能があり，何がどう生かされていて，何が問題とされているかについて検討した．インターネットオークション市場における評判システムは今最も注目されている分野の一つである．インターネットオークションでは，物品がネット上で売買されるため，自分の取引相手がきちんと商品を送ってくれる相手か，またはきちんとお金を支払ってくれる相手かという情報は，非常に重要となる．従って，オークション開催企業は，顧客が安心してオークションに参加できるような環境を整えるため，さまざまな評価システムを取り入れ，取引が無事終了されるように管理している．以下に，主要なオークション企業の評価システム等の安全対策を示す．

ヤフーオークション

ヤフーオークション（以下ヤフオク）は日本において一番始めにインターネットオークション事業で成功しており，一番初めだったからこそ抱えた問題を解決して今に至っているため，安全の確保についてもいろいろな工夫がされている．開始当初は参加費無料でおこなっていたが，現在はセキュリティ確保のため参加者全員から手数料を徴収している．また，補償制度としては，落札価格が５０００円以上の取引について詐欺等にあった場合には５０万円を限度として被害を補償する制度がある．

- 評価
  ヤフオクにおける評価とは，取引相手に対する満足度について，落札者と出品者の両方がお互いを評価することである．評価内容は全ての利用者に公開され，他の利用者が取引を考慮する際の資料となる．また，オークションシステムから自動的に評価される場合もある．

- 評価方法
  評価方法としては三段階評価がおこなわれている．よい（+1）どちらでもない（0）わるい（-1）の三つで，同じ取引相手から何度も評価を受けた場合は，最新の評価のみが残ることになっている．また，出品者が落札者を削除した場合，自動的にシステムから評価を受けることになる．この場合，出品者が落札者を削除した要因を探って非があったほうにマイナスポイントが加算される．

- 公表方法
  一目で分かる情報として，”よい ”と評価した人数から悪いと評価した人数を引いた数が表示される．さらに，詳細を閲覧したいユーザには，よいと評価した人数，悪いと評価した人数がそれぞれ分かるようになっており，さらに詳細を調べると，最新３０００件までのコメントが閲覧可能である．コメントは３０００件を超えた次点で古い物から削除されるが，評価数値はどんどん加算される．また，過去のオークションにおける評価も数値は常に閲覧可能となっている．

Bidders

Bidders の評判システムは，系列のさまざまなインターネットオークションで利用されている．例えば，@nifty や goo のインターネットオークションは同一の評判システムを利用している．Bidders ではインターネットオークションの先頭を走るヤフオクと異なった売りとして参加料を無料としている．しかし，落札価格の５%を落札料として徴収している．補償制度としては，落札者が購入者が売り手の詐欺等により金銭的損害を被った場合に最高１０万円まで補償するという制度を持っている．

- 評価
  Bidders における評価とは，約束をきちんと守ったか，メールの返事が早かったか，親切だったか，感じが良かったか等と言ったような総合した評価から段階評価までさまざまな方法で取引相手を評価する物である．

- 評価方法
  ここでも，ヤフオクと同様三段階評価だが，とてもよい，よい，問題ありの三つの評価となっている．総合評価のほか，取引や商品について感想等自由にコメントを記述できるようになっている．評価期限は落札，購入決定から３ヶ月以内と決まったおり，この期間を過ぎると変更することもできなくなる．また，評価は義務ではなく評価する人の判断に任せられる．あえて評価をおこなわないユーザもいる．さらに，同じ相手から複数の取引があった場合には，最後に入力された評価だけを対象にしている．また，取引拒否申請が認められ，次点入札者の人と取引をした場合，お互いに評価をつけることができなくなる．

- 公表方法
  公表方法としては，とてもよいと評価された回数から問題ありと評価された回数を引いた数を総合評価とし，ニックネームの後ろにその数値が表示されることになっている．詳細評価は最近廃止された．

Live door オークション

- 評価
  Live door オークションでは，出品者・落札者の人々に取引終了後にお互いを評価してもらう仕組みをもうけている．

- 評価方法
  評価方法としては，オークション終了後に出品者･落札者の双方に対して，livedoor から落札終了メールが送られ，その中に，評価やコメントをおこなうページへのリンクが記載されているので，そこにアクセスして評価をおこなうことになる．それぞれ取引が終了過程になっていると，自分のマイページから評価をつけられるようになっている．これはきちんと取引が終了している状態になっていないと評価できない．また，自動評価としては，落札者が出品者によって一方的に削除された場合，オークションシステムから出品者にマイナスの評価がつけられることになっている．評価は，とてもよい，ふつう，要注意の三段階評価で，コメントが残せるようになっている．

- 公表方法
  ニックネームの横に，とてもよいと評価した人数から要注意と評価した人数を

引いた数が表示されている．さらに詳細をみたい場合，それぞれの数がわかり，さらに過去にその人を評価した結果が過去一週間，一ヶ月，半年と分けて表示されている．また，コメントは，取引商品と評価と共に公表されている．

なんじゃもんじゃ市場

なんじゃもんじゃ市場では，入札制限サービスをもうけている．出品者が評価され選別の対象とされるだけではなく，入札者も自分の持っているポイントが悪いと入札ができなくなると言うシステムである．

- 評価方法
  なんじゃもんじゃ市場では，５段階評価になっており，非常によい（+4）よい（+2）普通（+1）悪い（-1）非常に悪い（-4）の五段階になている．また，コメントは任意でつけることも可能である．

- 公表方法
  公表方法は，ニックネームの横に評価ポイントを公表するという物である．全てのポイントを加減算したポイントが評価ポイントになる．また，詳細をみたい場合には，それぞれの段階が何ポイントずつ入っているかをみることが可能であり，さらにコメントを閲覧することも可能となっている．

ぐるぐるオークション

このオークションは少し変わった評価方法を持っている．全会員は会員登録時にセキュリティレベルという数値（デフォルトは１００）を持っており，何らかのトラブルが起き，トラブル登録されるとそのセキュリティレベルが下がり利用が制限されるという物である．

- トラブル登録
  オークション終了後のトラブルを解決するためのシステムで，取引終了後７日以上たつと利用可能となる．取引相手に不満があった場合，その問題をトラブル登録システムに登録すると，登録された相手のニックネームにダークぐるぐる君マークという物が付き，そのマークは取引危険相手として認識される．このマークは問題がきちんと解決するまで外されない．よって，このマークには問題あるユーザの入出品を止める威力があるとされ，またこのトラブル登録をおこなうのはユーザの任意なので，安易に利用することはさけたほうがいいとされる．

- 闇鑑定
  トラブル登録のシステムとは別に，闇鑑定というユーザ任意のボランティアで運営された機関があり，この機関は出品されているアイテムを鑑定し，アイテムが違法・詐欺等の問題がある場合，出品者が無駄に法律で裁かれないよう注意するシステムである．このシステムに引っかかった商品は，アイテムを削除するか，異議ありのコメントを登録する必要がある．削除すればリストから外されるが，異議ありの場合，法律で罰される場合があるとして再調査される．

以上のように，現在のインターネットオークション市場では，さまざまな評価システムが利用されている．ヤフオクが参加無料から有料にした際，競合他社は無料にす

ることで顧客を得ようとしたが，結局は参加料を払うことによってより安全が確保されるなら支払いをしたほうがいいというユーザが多く一時自分の市場をヤフオクから他へ移したユーザが結局戻ってきたという例もあったことから，ユーザがセキュリティに対して大きな関心を持っていることがうかがえる．

2.3.2 ネットオークション等の評判システムとの違い

以上が既存の評判システムであるが，これをそのまま本研究で想定している，個人向けサービスに対するものとして利用することが可能かどうかを考えると，ネットオークションの際に求められる評判情報と，個人向けサービスにおいて求められる評判情報との違いを明確する必要があるという問題が浮上した．

ネットオークションでは，一つの取引が終了した時点で，商品提供者と購買者がお互いの取引き状況について評価することが可能である．また，第三者が必要とする情報もこの取引がうまくいく相手かどうかという点だけである．しかし，本研究で必要としている評判システムではこうはいかない．

評価対象

ネットオークションにおける評価対象は，取引相手としてどうかという点だけだが，今必要とされている環境では，サービスのクオリティはどうか，個人情報の取り扱いはどうか，自分に適したサービスであったか等さまざまである．一回サービスを受ける毎にこれら複数の項目に対して評価をしなければならないのは，手間であり，せっかく個人情報の自己管理を自然に手間をかけずにおこなう方法を考えているというのにこれでは意味がなくなってしまうのである．また，評価時期についても違いが生じる．ネットオークションにおける評価時期は，取引終了直後で何ら問題はない．しかし，本研究において対象にしているようなサービスは何度もサービスを受けることによってよりユーザに適したものになっていくものであったりするので，評価を下す時期をいつにするかという点が非常に難しいのである．

さらに，評判システムそのものの信憑性が疑われる可能性があるという問題をもっている．ネットオークションでは，評判システムを提供している環境と，評価対象は完全に異なるものである．また，ヤフオクを信頼していれば，ヤフオクが提供する評判システムも信頼のおけるシステムとして認識されるが，本研究における評判システムは，第三者が評判システムを提供するにしてもその第三者を信頼できるかどうかという問題が残るし，サービス提供側が評判システムを管理すればそれはそれで公表情報には悪い情報を載せないようにしているのではないかという疑いが残る．従ってこの既存のシステムの導入することを検討する際にも信頼性という概念が重要になってくるのである．これについては，論点３－３で信頼性で論じている．しかし，今回の場合は，信頼性という概念の問題だけではなく，先に述べたようにさまざまな異なる要素が存在しているため，個人向けサービスを評価するという用途において，現在インターネットオークション市場で利用されている評価システムを利用することは難しいと判断した．

そこで，皆がいちいち評価を下すのではなく，ネット上の掲示板等で記されている評価や，個人の日記等で記されている評価等を利用して評判情報を取りまとめること

はできないかと考えた．これが，評判情報として求められている二つ目の要素である口コミ情報になると考えた．実際にそのようなことをおこなっている研究があったのでそれの詳細と，そのようなシステムを利用する際の注意事項を次節で論じる．

2.4 論点１－２－２：口コミ情報的な評判システム

評判システムの必要性は今後ますます増加していくと考えられるが，誰がどのように評判システムを作ることが一番信憑性の高いシステムが作れることになるのかを考えると，きちんとした答えが出せないのが現状である．そこで，新たに一から評判システムを構築するのではなく，現在インターネットという大きな空間に無数にあるさまざまなデータから必要な評判情報を取り出し，解析することで，何らかの評判を得られないだろうかと考えた．

そもそも評判とは，口コミ情報的なものであり，あえて意識的に評判を作るのではなく，ユーザが自分の利用経験をもとに思ったことを人に話したことがきっかけとなってそのものの評判として伝えられたりするものである．オフラインの環境では，口コミという形態になるが，オンラインであれば例えば日記に書いたことが広まってということになってもいいと思う．口コミの場合は実際に相手に話をするのだが，オンライン情報の場合にはそうはいかない．実際に何らかの情報を得たいと思った人が検索エンジン等を利用してそれについての情報を探すのである．

しかし，ネット上の莫大な情報量の中から，自分が必要としている評判情報を検索するのはなかなか難しいことである．実際に検索エンジンを用いて，キーワード入力から評判情報を検索しようとしても，評判を探したい対象の名前のみをキーワードにすると，大抵そのもの自体の情報が検出されて評判情報をヒットさせるのは難しい．例えば，レストランの情報であったら，レストランの名前と一緒に「おいしい」とか「まずい」といったようなキーワードを入力すると，日記等に書かれた情報がヒットすることがある．しかし，このような付属のキーワードはカテゴリ毎に異なるものだし，それで全ての情報がヒットするわけではない．しかも，ヒットした情報全てを調べるのは非常に時間のかかる作業であり，また全て調べたからといって必ず望んでるような結果が得られるとは限らない．そこで，このような一連の流れを自動でおこなってくれるようなシステムがあったら良いのではないかと考えた．

調べた結果，現在，blogWatcher というネット上の日記形式のサイト全てをクローリングしてその内容を解析するシステムがあった．このシステムは，キーワード別にカテゴリ分けをおこなうことで，キーワード検索をすると，ネット上の日記でそのキーワードを記述している全てのサイトを見ることができる．さらに，サイトの内容解析をしており，内容的にそのキーワードに対するポジティブな意見を述べているかネガティブな意見を述べているかを判断し，それぞれの量が折れ線グラフで分かるようになっている．

2.4.1 blogWatcher の評判情報

blogWatcher の詳細に関しては，ホームページ [8] に記されているが，問題点を考える上で必要であるので，概要を記す．

このシステムでは，blog 形式で書かれた日記以外の日記も判別可能としている．こ

れは，html 解析をおこなうことで特定の条件に当てはまったサイトを blog 形式で作成されていなくても blog として認識することにしているからである．特定条件とは，

- 日付情報が含まれている
- 日付が記事の上部にある
- 日付部分は規則正しく書かれている
  - 日付部分に関してタグの係り方は一定である
  - 日付の書き方も一定である

である．

このようにして blog として認識されたページは記憶され，日々のクローリングで更新されたページがあればそのページをもってきて内容解析することが繰り返される．キーワードのみでそのキーワードが記されたページ全てをもってくることもできれば，その評判を知りたいということであれば，そのキーワードが書かれた前後にポジティブな内容を示すような単語があるのかネガティブな内容を示すような単語があるのかを解析し，それぞれの量が一目で分かるようなグラフで表されるようになっている．

従って，既存の情報源を利用して評判を作るというのは一から作ることを考えるより現実的だと言える．しかし，このようにネット上の全ての日記内容を用いて評判情報を作るということを考えると，一つ一つの情報に対する責任が重くなることも考えなければならないのではないだろうか．日記というものは，何かを評価しようとして書かれるものではなく，自分の一日を記しておくためだけであったりすることが多い．しかし，ネット上にある限りそれは多数の他人から閲覧可能であり，場合によってはそれによって他の人の購買意欲を高めたり低めたり，何らかの影響を与える可能性があることは否めない．とはいっても，実際に自分のページに他人がアクセスする可能性は自分がアドレスを教えていない限りあまりないと考えていいわけだが，このシステムを稼働させることにより，自分の日記が他の人に影響を与えることが大きくなることは確実である．

ネット上で公開している限り，その内容には自分で責任を持たなくてはならない．いくら自分が思ってることを書いているだけだとしても，それが公の人に公開され影響を与える情報となると，内容によっては，相手から訴えられることもあることを忘れてはいけないのである．

この問題に関しては，次節で詳細に論じることにする．

もう一つ考えるべきことは，ネット上にある情報というのは必ずしも必要最低限の量が確保されているとは限らないという点である．項目によっては，多くの人がそれについての情報を提供している可能知れないが，項目によってはそんなにネット上に十分な情報がないこともあるかもしれないということである．自分が欲しい情報に関して十分な情報がなかった場合，他に評判情報を探す手がなくなってしまう可能性がある．

まず，どんな情報に関して多くの情報があって，どんな情報に関しはないのかという点を把握する必要がある．

2.4.2　現状の評判情報掲載率について

上述したように，キーワード検索はまず始めに手をつけるべき項目であるが，同時に考えなければいけないのは情報量の偏り具合についてである．インターネット上の評判情報は，誰もが掲載しているわけではなく，また，どこかで強制的に実行させているものでもないので，項目によっては情報量が少ない場合もある．そこで，インターネット上にある情報を利用して評判システムを構成することが可能であるかどうかを検討するためにも，どのような項目にどの程度の情報が寄せられているかについても調べる必要があると考えた．情報量が多い項目のほうが情報量の少ない項目より多く評判情報が気にされるとは一概に言えないことなので，なぜ情報量が多いのか，またなぜ少ないのかについても検討していく必要がある．また，これは日記情報のみならず，掲示板的情報源に関しても調べる必要がある．

比較的情報量が多い項目

掲示板等で討論がおこなわれるような内容に関しては，日記等を見ても評判に関する情報が記されているように感じられる．例えば，レストランや旅館等に関する情報である．店舗が公表しているホームページの情報を初めとして，その情報と実際に訪れた人が感じた対応に関するギャップについてだとか，紹介ページだけでは表しきれないサービスに関する情報等，さまざまな情報が公開されている．

ネットに公表された情報があると，その情報が他の情報を呼ぶのではないかと考えた．何らかの情報が公開されていると，その情報を見た人が当該情報を基に実際に体験する．そこで，感じたギャップや情報の正確性をまたネットにのせるという感じでどんどん情報が増えていってる．これは，論点１－２の頭で論じたようにな要因により評判情報の掲載が促されているからであることを証明している．

一方，ネット上に何も情報がない項目に関しては，ユーザもなかなか情報を掲載しにくいようである．自社のホームページを持っていないな企業に関しては，持っている企業と比べて著しく情報量が少ない．

比較的情報量が少ない項目

上記で記した，情報量が多い項目に関する定義が正しいとすれば，サービス自身がネット上に情報を掲載していないような項目に関しては，評判情報が少ないの考えられる．例えば，同じ車というカテゴリの情報を検索しようとしても，大手車メーカの情報は多く掲載されている物の，車の部品を担当している工場や下請け企業に関する情報は評判としてはさほど掲載されていなかったりする．

また，全体的に利用者の数が少ないと必然的に情報量も少なくなる．プログラミング基盤に関する情報にしても，主流な基盤に関しては詳細な情報とともに，利用し易さ，利用するにあたっての情報が多々掲載されている物の，さほど主流ではない基盤を利用するとすると一気に情報量が減少する．

さらに，インターネット上に評判が掲載されるかどうかということは，世論にも大きく関係している．例えばオリンピックの時期にはオリンピック関連の情報が集中的に掲載されるが，終わると途端に情報量は激減する．また，近頃起こったある車メー

カの故障に関する情報も，その話がテレビ等で頻繁に伝えられている時期は，ものすごい量の情報がインターネット上でも交わされていたが，最近それも収束してきた．このように，インターネット上の情報というのは，世論の流れに大きく関係している．

しかし，勿論それだけではなく，インターネットだからこそ検出されるようなレアな情報も持ち合わせているのが特徴である．情報量が多いか少ないかは別として，浅く広い範囲の情報をも持ち合わせている．従って，評判という大きな形では表すことのできない情報量かもしれないが，基本的に情報を探すことが難しいと思われるようなカテゴリの情報も検出可能である．

従って，既存の情報から評判情報を作り出すというシステムを構築する上では，評判情報にするために一定量の情報が必要とされるが，それとは別に，小さなコミュニティの中での評判情報という物ができてもいいと考える．一般論として提供するには情報量が足りない場合でも，小さなコミュニティの中の意見としてなら有効利用できることがある．

インターネット上の既存の情報から評判情報を作り出すということを検証する際には，一般論として提供する情報と，一般論としては提供することはできないが，他の形で提供することのできる情報があるということを把握した上で，全ての情報が有効利用されるよう検証すべきであると考える．

2.5 論点１－２－３：blog の内容に対する名誉毀損問題

基本的に blog はインターネット上の日記であり，作者個人の感情や興味によって自由に書かれる場だが，一般の日記と違って他人からアクセス可能であり，その内容によって他者の意見を動かすことも可能なことから，場合によっては名誉毀損や信用毀損に当たる可能性がある．名誉・信用毀損と言論の自由の間には難しい関係があるが，この blog の内容から評判を作り出すことが考えられている以上考えないわけにはいかない要素なので，本節では起こりうる法的問題としてどのように対処すべきかを論じる．

まずは，どんなことが名誉・信用毀損に当たるかという点である．名誉毀損に関する詳細は，付録 D に記載した．概要として，名誉毀損には，刑事と民事の二種類がある．刑事の名誉毀損罪とは,「公然と事実を摘示し，人の名誉を毀損した場合に成立」と定められている．しかし,「事実の有無，真偽をとわないが，公共の利害に関する事実に関係することを，専ら公益目的で摘示した結果，名誉を毀損するに至った場合には，その事実が真実である場合は処罰されない」とある．また，民事においては,「原則として，客観的な社会的評価がこの類型によって保護され，単なる主観的名誉感情の侵害は含まれない」とある．さらに，事実を伴わず評価・判断をすることによって社会的評価を低下させたような場合には，侮辱罪が適応されるので注意が必要である．

日記の場合，通常名誉や信頼を毀損しようとして何らするものではないので，当てはまりにくいと考えられるが，日記等によって評判情報を構築することが一般的になってきたらそれを悪用して評判を操作しようと考える人が出現するであろうと考えられるので，そういったことへの対処法も検討すべきである．

実際に，ネット上で人権を侵害されたという被害者は年々増加しており，これらの多くは，法務省が援助して被害者本人からプロバイダに直接削除の依頼をおこなうこ

とで解決されてきたが，件数の増加に伴い法務省から直接削除依頼をおこなうためのプロセスが考えられた．現状の，削除依頼をおこなうためのプロセスは以下の通りである．

2.5.1 法務省が削除依頼をおこなうときのプロセス

被害者以外の第三者から法務省に対して人権侵害の指摘が寄せられた場合等，各法務局・地方法務局において，

- 人権擁護上，看過できない事案であるかどうか
- 被害者自らが被害の回復・予防を図ることが諸般の事情を総合的に考慮して困難と認められる事案かどうか

を検討．さらに法務省人事擁護局による再検討と認証を受けた後に，各法務局・地方法務局の局長名でプロバイダーに対して削除依頼をおこなう．

2.5.2 プロバイダがページ削除をおこなうときのプロセス

法務省から削除依頼を受けたプロバイダは，

- URL 等の侵害情報が特定されていること
- 侵害情報をプロバイダ自らが確認し，ガイドラインの判断基準に照らして，他人の権利を不当に侵害したと信じるに足る相当の理由があることが明白であること

等の条件が全て確認できた場合に，実際に情報の削除をおこなうかどうかの判断に移る．

実際には，ガイドラインに法的義務はないので，最終的に削除されるかどうかはプロバイダの判断に任されることになる．
しかし，blogWatcher の用なシステムが主流になると，内容解析の精度を上げることにより，内容が更新された次点でその内容が人や企業の名誉や信頼を毀損するものと成りうるかどうかの判断もできるようになるのではないかと考えられる．

2.5.3 プロバイダ責任制限法

上述したように，法務省等から削除依頼を受けたプロバイダは一定の条件かでサイトの削除をおこなうことが可能である．その詳細規定について定めているのがプロバイダ責任制限法である．詳細は最後の付録 E に添付するが，概要をここに記すことにする．

趣旨

この法律は，特定電気通信による情報の流通によって権利の侵害があった場合について，特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示を請求す

る権利について定めたものである．これは，特定個人の民事上の権利侵害があった場合を対象としている．

ここで言う，特定電気通信とは，　不特定のものによって受信されることを目的とする電気通信の送信のことであって，インターネットでのウェブページや電子掲示板等の不特定のものにより受信されるものが対象となっている．ただし，放送に当たるものは，放送法等での規律があるため，対象外となる．また，特定電気通信役務提供者とは，特定電気通信の用に供される電気通信設備を用いて他人の通信を媒介し，その他特定電気通信設備を他人の通信の用に供する者のことである．具体的には，プロバイダやサーバの管理・運営者等が対象となる．

概要

この法律では，サイト内の情報に関して，名誉毀損や信用毀損等でプロバイダ側にサイト情報送信防止措置を求められた際，プロバイダ側がどのような対処をする権利があるかについて定義されたものである．基本的に，そのような請求があり，その内容が人の権利を侵害していると思うに足りる理由があった場合，その情報の発信者に対処をおこなう旨を通知し，反論がなければプロバイダ側が勝手に送信防止措置をとっても良いということになっている．また，このようにきちんと手順を踏んでおこなうことで，発信者側から「言論の自由」の侵害等で訴えられることはないとしている．

2.5.4　まとめ

本節のまとめとしては，ネット上で個人の日記を記す際，ネットで公開しているとはいえ，不特定多数の人がアクセスすることはないだろうと思って書いていることであっても，blogWatcher のようなシステムが一般化した際には，一つ一つの情報は評価を構成する上で重要な要素の一つとなることを認識しなければならないということである．また，自分からどこかに登録して検索エンジンに係るようにしなくても，全ての blog の内容をクローリングするようなシステムが増えれば簡単に検索に引っかかって公の人の目に触れることになることも認識する必要がある．

この問題は，自分の権利が他人の権利を侵害する恐れがあるという問題で，新しい技術が導入されることで，その問題が強調されてしまうというものである．既存の情報源を利用して新しい情報として提供することができるようになると，氾濫する情報を整えることにもなり，使い方によっては非常に役に立つものになると考えられるが，前にも述べたように新しい技術の導入と検討する際には，それに伴って新たに非技術的な視野からの考察も必要になるのである．

2.5.5　論点１－２まとめ

街を歩いているだけで数えきれないほどのサービスの恩恵を受けられるような環境が整った場合，どのサービスが自分に合ったサービスなのかという情報を把握するのが非常に困難になってくる．また，見ず知らずの相手に自分の個人情報を提供していいものだろうか，本当にその情報が必要なのだろうかといったような心配も生まれる．そのような中で，何らかの方法で事前にそのサービスについての第三者の意見を知る

ことができたら，サービスを受けるかどうかの判断基準の一つになり，個人情報の自己管理の手助けになると考えた．

そこで，既存の評判システムの関する調査をおこなってみたが，それをそのまま利用するにはいくつかの問題が発生することがわかった．また信頼性の問題もあるので，既存の評判システムとは別のアプローチを検討することにした．それは，新たに評判を作るためのシステムを構築するのではなく，氾濫しているデータの中から必要な情報を抽出することから評判を作ることができないだろうかというものである．

このアプローチは既に研究されたものであったので，それの有効性を検討し，それを利用する上でどのような問題が発生するかについて調査をおこなった．技術的な問題としては，自然言語解析の問題がある．言語解析に分野の研究が進むことで，より忠実に評判情報を抽出することが可能となる．しかし，この分野の話は自分の研究分野と大きく異なってきてしまうので詳細は論じないこととする．実際に利用してみた感じでは，まだ完全に評判の情報を抽出することはできてないようなので，今後の自然言語解析の分野の研究に期待するところである．

また，実際にこれが利用されるようになると，一人一人が自分の掲載する情報に今以上に責任を持つ必要が出てくる．通常，特に人に教えない限りそうそう他人にみられることがないのが個人の日記サイトである．自分の書くことを他の人に知らせたいから書くのではなく，自分のためにただ記しているという人も少なくない．しかし，完全に全ての日記サイトをクローニングするとなると，自分の書いた情報が確実に第三者が何かを判断する際の基準になり得るので，そこで記した情報があまりに否定的だと何らかの問題に巻き込まれる可能性があることを把握しておくべきである．

自分にそんな気がなくても，名誉毀損や信用毀損になり得る情報を公開していたら，今以上にそれが公に発覚される可能性が高くなることを認識すべきである．実際に罰せられるのは，意図的に侵害した場合だが，意図的であるかないかという問題は証拠を立てられるものではないので，このようなシステムが主流になってくると，それを逆手に取って悪用しようとする人が出ることも考えられるので，簡単に罪になるならないを決めることができなくなることが予想される．現状では，どう対処したらいいか明確な対処法が考えられないが，とりあえず自分の提供する情報には責任を持たなくてはならないことを認識すべきである．

以上のような点を注意した上で，個人向けサービスが偏在する環境において，サービスを自分が利用するかしないかを判断する一つの基準として，現在ある情報の中から，また，今後自然に増加していくであろう情報の中から必要なデータを抽出することによって構成される評判情報を利用することを提案する．

2.6　論点２－１：グローバルな法的規制

グループ２は，技術的対策に対して非技術的対策が必要とされている論点である．まず初めは，グローバルな法的規制についてである．インターネット空間とは，国境のない空間なので，個人情報をインターネット上で取り扱うことを考える際には，グローバルな視点で検討する必要がある．というのも，国によって異なる規定があり，日本で許可してる範囲のことが海外で許されてなかったり逆に，日本で制限している点において，海外で許可されていたら，通信方法を変えるだけで悪用できてしまったり，外国からのサービスがうまく働かなかったりといった問題が発生してしまうのである．

技術の進歩に伴い，国境を越えた取引をおこなえる可能性が増加してきた．これは，さまざまなサービスが店舗というものを持つ必要がなくなってきていることから，国外の市場が簡単に入って来れるようになってきたからだと考えられる．従って，このような取引を適切におこなえる環境を整えるために，各国がプライバシ保護についてどのような見解で臨んでいるかを把握する必要が出てきたのである．

プライバシ保護については，OECD がガイドラインを作成しており，加盟国がそれに沿ってそれぞれの規律を作成するということになっている．以下に ”プライバシ各国現状 ”[9] に記述されている OECD のガイドラインの内容と概要，さらにそのガイドラインを受けて各国がどのように対処しているかについて記述する．

2.6.1　OECD

Organization for Economic Cooperation and Decelopment（以下 OECD）は経済協力開発機構のことで，フランスのパリに拠点をもつ．2000 年現在，30 カ国が加盟しており，先進国間の自由な意見交換・情報交換を通じて,「経済成長」「貿易自由化」「途上国支援」に協力することを目的として活動している．

当機構は 1980 年にプライバシ保護と個人データの国際流通についてのガイドラインに関する理事会勧告を採択している．個人情報の収集と管理に関しては以下の８つの原則が OECD プライバシガイドラインにおいて定義されている．

- 収集制限の原則
- データの質の原則
- 目的明確化の原則
- 安全保護の原則
- 公開の原則
- 個人参加の原則
- 責任の原則

当ガイドラインは，強制力はないが，グルーバルネットワークにおけるプライバシ保護に関するガイドラインは今後よりいっそう必要不可欠となるものであり，完全なる保護をおこなうためには全世界が一つのガイドラインに従う必要がある．

次に，OECD の８原則を受けて各国がどのような対応をしているかについて紹介する．

2.6.2 欧州連合の個人情報保護

EU としての，個人情報保護法としては，1995 年に発行された「データ保護指令」がある．この指令は，OECD の８原則を考慮した上で，加盟国間における情報の自由なやり取りを確立・維持するとともに，加盟国以外の国への情報の流れを管理・監視するために作られたものである．ヨーロッパは特に個人情報保護に関する考えが厳しいと言われている．97 年には,「通信部門における個人データ処理及びプライバシ保護に関する欧州議会及び理事会の指令」が発行され，さらに翌年に「データ保護指令」が施行された．

この指令では，十分なレベルの保護がおこなわれていない第三国への個人データの移動も禁止されている．さらに，EU 国民から個人情報を収集するいかなる会社もこのデータ指令に従わなければならないとしている．このように定義することで，異なる法を持つ相手にも対応しているのである．

2.6.3 アメリカの個人情報保護

実際，アメリカにはプライバシに関する包括的な国内法は存在していない．しかし，憲法ではプライバシは全ての米国市民の権利であることが定義されている．全般的な法がない代わりに，部門毎でプライバシを保護する形を取っている．また，民間部門でさまざまな規定がされている．

しかし，EU はきちんとした法が制定されていないとデータのやり取りをおこなってはならないとしているので，便宜上取引上のデータ移転を可能にするため，セーフハーバ契約を二年間の試行期間を伴って発行してもらっている．米国の各社が EU のセーフハーバの地位を申請するには，一定の基準に合致するような告示書を提出する必要がある．

2.6.4 アジアの個人情報保護

アジアにおける IT 先進国であるシンガポールでは，個人情報保護に関する全般的な法律は存在していないが，シンガポール最大のインターネット業界境界が，TRUSTe[3]のプライバシシールプログラムの支持を発表した．それに伴い，同協議会のメンバが多数導入した．さらに，ブロードバンド大国の韓国では，94 年に「公共機関により管理された個人情報の保護に関する法」を策定し，98 年には，アメリカと共にネット上での電子商取引を推進していくことを発表した．

2.6.5 GBDe

Global Business Dialog on Electronic Commerce（以下 GBDe）は，日本では電子商取引に関する国際ビジネス会議と呼ばれ，米国，欧州，アフリカ，アジア等各国の電子商取引に関わる主要企業１００以上が参集した企業同盟の会合である．GBDe では，課税問題や消費者信用，個人情報保護，知的財産権，電子認証とセキュリティ等電子商取引のフレームワークを構成する九つの項目を検討している．

[3]TRUSTe：アメリカでネットユーザから信頼を得ているサイトの信憑性を保証する制度・詳細は関連研究にて示す

個人データ保護に関するガイドラインは，OECD のガイドラインに基づいて以下の５原則が挙げられている．

- プライバシポリシの採用と実施
  コンプライアンス・プログラムの形式での履行，管理職や関係する社員の教育
- 個人データの収集の原則
  収集目的の明確化，オプトアウトのメカニズム
- 個人データの利用と開示の原則
  個人データの利用と開示は収集時の目的と整合的でなければならない
- データのセキュリティの原則
  責任の保証，個人データの保護
- データの質とアクセスの原則
  個人データの正確さの保証，データ主体のアクセス，修正，削除の権利

また，第一回総会においては，個人情報保護に関して，以下のような提言をおこなった．

1. 企業と政府は GBDe の五原則の促進とプライバシポリシの実施のために協力するべきである
   - 企業は業界にとって最善な個人情報保護手段を選択するべきである
   - めまぐるしく変化する電子商取引の世界において，政府の規制は必ずしも十分な個人情報保護手段とはならない，また，政府が国際間のデータ移動を制限することは，自由な流通の発展にマイナスの影響を及ぼす
   - 企業と政府は協力して GBDe の五原則の教育と促進をおこない，電子商取引に携わる企業のプライバシポリシの実施を保証することで，消費者が個人データ保護の重要性を理解できるようにしなければならない
2. 自主規制メカニズムの開発と使用の促進
   - 個々の企業はシール・プログラムか自主宣言プログラムかどちらかを選択する責任を負っている
   - 政府は自主規制を促進する役目を果たさなければならないず，インターネットにおける個人情報保護に関して，実世界における以上に厳しい規制を課してはならない
   - 企業と政府は協力して自主規制メカニズムを開発するべきである

ガイドライン発表にあたっては，OECD の八原則を基に作成しているものの，国家レベルのトップが検討している OECD とは異なり，実際にグローバルに業務を展開している各国の企業のトップが現状の技術や個人情報保護に関する世の中の流れを考慮した上で制定したものなので，より現実的なガイドラインになっていることを主張している．

また，GBDe が毎年おこなっているカンファレンスの提言書 [10] [11] [12] は，インターネットの普及に伴う課題等について提言をおこなっており，筆者が考えなければならないとしている部分と多く重複しているので，関連研究において詳細を紹介する．

2.6.6　論点２－１まとめ

インターネット上のプライバシ保護に関する問題というのは，もはや一つの国という単位で考えていては起こりうる問題に追いつかない状態になってきている．インターネット技術の進歩と，インターネットの普及に伴い，国境をまたいだ商取引が普及してきたからである．そこで，OECD のような機構がガイドラインを提言し，加盟国がそれをもとに自国での法制を検討するという流れが必要不可欠となっている．日本も，この機構には加盟しているので，日本における法案を検証すると，グローバルなガイドラインに従っていると言えるが，既存のいくつかの法案があるがために，まだまだ穴のある法案であると言わざるを得ない．

また，現在，主要各国もこの機構に加盟しているので，比較的多くの国の間でプライバシ保護について似たような法案が設定されているといえる．しかし，前にも述べたように，全ての国において一致した考えを持たないことには意味がなくなってしまうのである．

現状では，データ保護法とプライバシ保護法の関係性の結びつきが一つの問題となっている．例えば，ドイツでは，データ保護法はかなり厳格に規定されており，データの取り扱い方や収集方法，処理についての規定がされている．しかし，この法案とプライバシ法は結びついていないのが現状である．プライバシに関連する法案としては，通信におけるプライバシ法は存在するが，それだけでは必要な範囲を網羅することができないのである．

加えて，文化の違いも関係してくると考える．プライバシという言葉にさまざまな定義があることは序論で述べたが，この意味の違いには文化の違いも関係しているのである．実際に，日本に滞在したことのあるイギリス人の体験を基に，日本人とイギリス人のプライバシについての考え方の違いを表している人もいる [28]．高谷氏によると，日本人はまだまだプライバシという概念に対する認識が低いそうだ．”プライバシ ”という言葉を何か ”特別な秘密 ”のように解釈しているため，初対面の相手に家族の構成や，年齢等個人的な質問を当然のようにする．これは日本における今までの社会常識からいって ”他人に知られてはマズイ情報 ”ではないからである．しかし，イギリスから来た人にとってこれらの情報を初対面の人に聞かれることはプライバシ領域に踏み込まれる気がしてしまうのである．このような感覚に違いもグローバルに統一したガイドラインを制定しようとすることを妨げる要因の一つになってしまうのである．

このような文化の違いは，プライバシの保護の重要性や個人情報を外部に出すことに対する認識の違いも生んでしまうのである．例えば，日本では，家族構成や住まいが一軒家か住宅かといった程度の情報の提供には，たいして大きな抵抗は持たれないが，アメリカ人の友達はそういった情報は容易に外部に漏らすものではないという．また，子供が家に一人の時には電話に出る事自体危険だという意識を持った人が多い．これは，家族構成や住まいのタイプから何らかの犯罪の対処にされる可能性があると考えるからだそうだ．著者は，友達からそういった意見を聞かされて初めてそういった可能性は否定できないものだと考えるようになった．やはり長い間安全社会であるといわれて続けてきた日本では，犯罪に対する考え方がまだまだ甘く，従ってプライバシの保護という要素に関しても，十分に理解しきれていないように考えられた．

アメリカのようにきちんと法として規制されていなくても，国民がその重要性・危険性を認識しているという状況の方が，日本のようにほうとしての規制はされているものの，国民が危険性を十分に理解していないという状況の方が危険であるといえる

かもしれない．

以上からも分かるように，国によってプライバシ法をどのように組み合わせるかという問題は，同一のガイドライン発行機構に加盟していても異なってしまうのである．これは，上述したように文化の違いによっても異なる上，インターネット利用の度合いによっても異なってくるのである．例えば，日本においては携帯電話の急激な普及に伴って，モバイル機器を利用したサービスの提供等が急激に増加した．これに伴い，モバイル機器を通じて個人情報を取り扱うという機会が増加し，それに伴いデータ保護とプライバシ保護をよりいっそう明確に規定する必要ができた．一方，ドイツにおいては，自分が在独していた経験からいっても日本ほど携帯電話が普及していなかったり，インターネット普及率も異なるように思えることから，それほど急いで法案を検討する必要がなかったのかもしれない．

このように，いくら世界中で検討しなければならない問題だとしても，実際に自国の問題とならないとその議題に対する真剣度が上がらなかったり，国民一人一人が十分認識しているからあえて法的に規制する必要がなかったりといったように異なってくるのは仕方のない事実である．しかし，複数の国をまたいだデータの流通が盛んになってきている今，各国が個別に検討してきた問題が全体として考えられ始めてきたといえる．これは，GBDe 等が構成され，さまざまな企業の代表者が，国別ではなく同一業界として一つの問題に対して検討を始めていることからも分かる．

未だ，皆が認める一つの答えは出ていないが，一企業のガイドラインが一業界のガイドラインとなり，国の法案となって，世界に向けるガイドラインとなり，統一の法案となることを目標に進んでいくためには，GBDe 提言書でも論じられているように，一個人がプライバシ保護についてきちんとした知識を持って臨んでいくことが必要不可欠である．文化の違いに基づく考え方の違いを統一することは出来ないが，個人情報の取り扱いに関して十分に関心を持ち，プライバシの保護を自らきちんとおこなうことの重要性を認識させないことには，統一したガイドラインを完成させることができないと考える．

2.7　論点２－２：セキュリティ

二つ目の非技術的対策が必要とされる論点とは，プライバシ保護のために技術者達が一番始めに検討を始める情報セキュリティである．セキュリティ対策に関しては，さまざまな方面の研究者が，さまざまな方法で対策を立てている [14]．個人情報保護のために，企業側がすべきこととして，収集した個人情報が安全に管理されているという状態を構築することだと論点１－１において論じた．また，収集する際にハッキング等によって悪意のある人に取得されないような環境を整えるのも企業側の役割である．では，初めに，既存の解決策としてさまざまな研究がされている技術的対策について考える．

十分なセキュリティ対策のもと情報を管理するためには，どのような状態を構築する必要があるのかについて検証する．

まず企業は，リスクを理解することが必要である．NPO 日本ネットワークセキュリティ協会 [13] [17] では，リスクを検証する際重要となるキーワードは二つあるとしている．脅威と脆弱性である．脅威とは攻めるものの強さであり，脆弱性とは守るものの弱さである．つまり，脅威は自らが管理できない対象が与える影響の大きさであり，脆弱性は自らが管理すべき対象の不備のことなのである．セキュリティについて対応する際には，この両サイドから検証する必要があると考えられる．脅威の大きさに対して，脆弱性を十分に低くする必要がある．

では，セキュリティを考慮する上で重要なキーワードとは何であろうか．以下の要件を中心に検証していく．

1. 機密性：許可された権限に従ってのみ情報にアクセスできるようにする
2. 完全性：データが常に完全であるように，欠落，重複，改ざんを防ぎ，正当性，正確性，網羅性，一貫性を維持できるようにする
3. 可用性：情報システムが必要なときにきちんとサービスを提供できる状態を維持できるようにする

それぞれ，機密性，完全性，可用性を高めることで，脆弱性を低くすることになる．また，これら三つの要件を組み合わせ，さらに三つの要件が生まれる．

- 機密性と完全性：アクセス制御
- 完全性と可用性：否認防止
- 可用性と機密性：識別と認証

従って，初めの三つの性質のうち一つでも脆弱性の高いものがあると全体的バランスが崩れ，セキュリティの確保が難しくなるのである．

脅威になり得る候補としては大きく分けると次の三つが考えられる．

- 自然：物理的破損
- システム：誤作動
- 人間：悪用

以上のことを考慮した上で，セキュリティ対策として検証が必要な要件について論じる．

2.7.1 技術的対策案

まず始めに，アクセス制御を正しくおこなうには，きちんとした認証技術が確立されることが必要不可欠である．これによって，機密性を高めることになり悪質な改ざん等を防ぐことが可能となる．従って，完全性を確保できるようになり，可用性を高められるのである．では，現在どのような認証技術が利用されているのか，またその技術利用における現状の問題点はどのようなものかについて検証する．

認証技術

一言で認証といってもさまざまな種類がある．ある機能を利用しているユーザを単一の識別子によって特定するための ”識別 ”，申請通りの識別名をもつユーザであることを確認するための ”認証 ”，本物であることを公的に証明するための ”証明 ”等である．その上で，識別名の他に属性情報を持ち，その属性情報に従って正しい権限が与えられることになる．

識別や認証は，なりすまし[4]等による不正行為を防ぎ，機密性と完全性を高める．認証の基本は，本人確認にある．認証方法は，次の三つの種類に分けられる．

1. 記憶
   パスワードや暗証番号等，本人しか知らない情報をもとに認証をおこなう
   - 誕生日や，電話番号等他人が容易に想像できてしまうような情報を使うと危険
2. 持ち物
   カード，印鑑等本人しか持っていないとされるもので認証をおこなう
   - 落としたり，盗まれたりすると危険
3. バイオメトリックス
   指紋，声紋等本人そのものの特徴をもとに認証をおこなう
   - 現在の技術では，複製は困難とされているため，比較的確実である
   - 技術を取り入れるコスト面にはまだ問題が残る

以上のように，さまざまな認証方法が利用されているが，それぞれ問題を持っており，完全な認証というものはないというのが現状である．しかし，電子商取引が普及するに従って，認証技術はより重要な技術となり，認証基盤がきちんと確立されることが必要不可欠となりつつある．そこで，現在それぞれの弱点を克服すべくさまざまな対処法が検討されている．

例えば，一番普及しているパスワード等の記憶に関する技術においても，定期的な変更の義務付けや，暗号化，ワンタイムパスワード[5]導入等が検討されている．また，暗号化技術等を利用して公開鍵技術を取り入れることによって，取引相手を認証しようという試みもあるが，これもまた ”なりすまし ”等の問題が解消されない限り，重要な取引の際の証明としては利用不可能である．そこで，”なりすまし ”防止のため，電子商取引市場では，デジタル認証，デジタル証明書といった技術の導入によりセキュリティを強化しようと試みている．

[4]なりすまし：当人であるかのように偽って操作をおこなうこと
[5]ワンタイムパスワード：一度しか利用できないパスワード

デジタル認証，証明書

デジタル証明書とは，証明書の所有者を識別する妥当性検査をするデジタル信任証のことで，パスポートのようなもののことである．電子商取引市場においては，決算等の際に個人を確実に認証する必要があり，そのための手段として用いられることが検討されている．オフライン環境においては，直筆の署名によって個人を特定しているが，オンライン環境においてそれはできないことなので，このデジタル認証を繁栄させることによって，新しい法制度が用いられ，デジタル証明書が直筆の署名と同様の価値を持つことができるようになることが，望まれている．では，そもそもどのようにしてこのデジタル証明書は発行されるのかということについて以下に示す．

まず，証明書を発行するのは，認証局 (以下 CA) と呼ばれる信頼された第三者グループである．各 CA には，証明書を発行するために必要とする識別情報を判断するポリシがそれぞれ存在する．そのポリシによって，証明書を発行する際にユーザが提供しなければならない情報が異なるのである．証明書はそれを利用する用途によって重要度が異なるのである．例えば，個人情報の取り扱いに関するときにはいっそう厳重な審査が必要とされるのである．

認証局は，基本的に三つの機能による構成されている．

1. 認証局
   電子証明書を登録・発行管理する

2. 登録局
   電子証明書を登録認証する

3. 発行局
   登録局が認証した証明書を発行する

これら三つの機能によって実現するシステム基盤を公開鍵基盤（PKI）と呼ぶ．このような基盤を整えることが今後のユビキタス社会にとって必要不可欠なのである．

認証技術と同じ位重要なセキュリティ対策として暗号化技術が挙げられる．ネット上で情報を取り扱う場合には，通信途中のセキュリティも確保しなくてはならない．管理してある情報に関するセキュリティ対策として認証技術をあげたが，そもそも管理される以前の通信段階で情報をハッキングされたら意味がなくなってしまう．現状で検証されている暗号化技術としては次のような技術が挙げられる．

暗号化技術

暗号化技術とは，古代から敵に通信内容を解読されないようにという目的でさまざまな手法が考えられてきた．今日においてもその目的は変わっておらず，現在は主にインターネット上のデータ通信の際に通信を妨害しようしたり，データを改ざんしようとしたりする第三者からデータを守るために利用されている．暗号化の効果としては，情報を不適切な人に見せないようにできることから機密性の保持が可能とされ，不正な改ざんを防止できることから完全性を保つ手助けができることがあげられる．三大要素の三つ目である可用性に関しては，直接暗号化技術が役立つことはない．

では，実際にどのように暗号化をおこなうことで効果を保つことができるのかということに関して検証する．まず，暗号化技術に関して検討する際，一番に頭に浮かぶ

ことは，破られない暗号はないということである．暗号化技術は，平文[6]を暗号化して，復元するためのものなのである．暗号化するために，鍵を用意して，また復元するために，鍵が必要とされるのであるが，元は平文だったものを暗号文から復元させるのは，時間はかかるものの復元不可能な暗号文はないであろう．しかし，さまざまな技法を組み合わせて利用することで，簡単には復元しにくくすることが可能である．

一般的に利用されている方式は，公開鍵暗号方式[7]と共通鍵暗号方式[8]を組み合わせて利用する方式である．この二つの方式を利用することによって，単独利用のみで暗号化をおこなうより違法な復元が難しくなるのである．まず，文書 X を B さんに送りたい A さんは，共通鍵 C を用いて文書を暗号化する．そして，共通鍵暗号方式は，暗号化した鍵を相手に渡さなくてはならないので，鍵を B さんの公開鍵で暗号化して送信する．すると，B さんは自分の秘密鍵を用いて鍵 C を復元し，その鍵を利用して文書を復元できるようになるのである．このように，二重の暗号化をおこなうことでより強固な暗号文を作成することができるのである．

しかし，初めにも示した通り，絶対復元不可能な暗号は存在しないので，どんなに時間を割いてでも復元したいほどの情報に対しては，その情報を何が何でも第三者に知られたくない場合，ネット上での通信は避けたほうがいいとされる．

2.7.2 非技術的対策案

では，既存の技術的対策では補いきれない部分をどのように非技術的対策で補っていくかという問題についてである．前に記述したように，個人情報を違法に取得したり，正規の経路以外から取得した情報を勝手に流出させることが違反であることは既存の法案で定められている．しかし，ここで問題にしたい点は，現在セキュリティ対策として研究されている手法が補えない問題に関してである．つまり，認証技術にしても暗号化技術にしても，新しい技術が登場すると，それを破るための新しい技術も登場してしまうという問題についてである．これに関しては，新たに法的な規制が必要とされると考える．

この問題は，オフラインの世界における ”鍵と鍵師 ”の関係に似ていると考える．新しいタイプの鍵が生まれると，合鍵を作る技師はそれ用の新しい手法を構築し，鍵の複製を可能にする．また，何らかの状況で鍵をなくしたりした際に，鍵を開けてくれる技術者も常に新しいシステムに対応できるように新しい手法を生み出している．これらの技術は，悪用されると大きな犯罪を生む可能性がある．しかし，必ずしも悪用するためのにのみ使われる技術ではないので，その技術の登場を規制することはできないという問題がある．

この話と同じ問題が，セキュリティシステムにおいても発生する．暗号化技術に関しては，解けない暗号はないという話をしたが，認証基盤においても同じようなことがいえる．新しい認証システムが開発されても，それを破る攻略法が必ず生まれるのである．現実社会における鍵の場合，新しい鍵を開発する際，ベテランの鍵師の人に一定の時間内で開けられるかどうか試してもらった上，決められた時間内に破られなかった場合一定の強固が保証されることになる．セキュリティシステムにおいても同じことがいえると思うが，時間が無制限にあったら決して破れないシステムはないと

[6]平文：暗号化されてない状態の文章

[7]公開鍵暗号方式：一般に公開されている X さんの公開鍵 A で暗号化された文書は X さんだけが保持している秘密鍵 B がないと復元できない

[8]共通鍵暗号方式：暗号鍵 C で暗号化された文書はその鍵 C でのみ復元できる

考えた方がいい．では，そのような状況の中でただただ諦めるのかというと，それでは意味がないのである．

そこで，新たな法的規制が必要だと考える．ここで必要とされるのは，セキュリティ対策用に十分な手順を踏んで開発された技術に対し，それを破る技術を公開することに関する規制である．新しい技術に対し，なんらかの対抗策を考えついたり，構築したりすることができたとしても，それをむやみにやたらに公開することを禁ずるのである．システムを破る手法があるということは，システムに脆弱性があるということであり，それを公表することによってシステムを開発する側としては新たな課題として対策を立てることができるので，利用の仕方によっては必要なことであるが，この脆弱性をむやみに公開することは，その脆弱性に対して対策ができる以前に攻撃する機会を不特定多数の人に提供することになり，非常に危険なことに成り兼ねないのである．脆弱性があるという事実が発覚したら，該当者に対し，対策を施すよう早急に促すことは必要だが，その方法を十分に考慮しなくてはならないということである．従って，そういった場合にどう対処すべきかというガイドラインのようなものが必要となり，その上で，悪意をもってそれを公開したりすることを制限するような法案が必要なのである．また，”悪意をもって ”というように表現したが，実際に悪意があるかどうかはみて判断できることではないので，そういったことも考慮した上で検討する必要があると提言する．

最後に，一般消費者の意識についてである．個人情報に関する保護技術や，プライバシ保護のための法制度の見直しは少しずつではあるが進んでいると言える．しかし，一般消費者が持つべき責任についてはまだまだ検討の余地が残されている．セキュリティ対策において一番重要であるのにも関わらず一番対策が不足している点は，この一般消費者の意識の問題であると考える．

2.7.3 意識改善の必要性

自分の個人情報は，自分で守るということについては論点１－１で示した．その際，自己管理を進める上で必要であると考えられる技術の提案もおこなった．そして，技術だけでは保証できない点については法制度の見直しが必要であると論じた．次の概念は，一般消費者自身の意識改善についてである．

セキュリティを確保する上で，一番重要な点は，一人一人がセキュリティ確保の重要性を理解し，そのための努力を惜しまないことである．どんな強固なシステムが開発されても，それを取り入れなければ意味がなく，ネット社会は，境界のない社会なので，一人の消費者がセキュリティを確保していないだけで，全体が崩れる可能性がある．

従って，一人一人の意識改善が求められる．例えば，今までは，”結果よければ全てよし ”主義だったところも，”プロセスが妥当であれば免責される ”という考えに変える必要が生じるのである．自分に害が出るまでことの重要性に気がつかない人も居るが，それでは遅いということを認識してもらいたい．論点３－１で説明するアンケートに協力していただいた人に意見を聞いた時にも，自分に害のない範囲であれば個人情報であれなんであれ勝手に使っておいてもらった方がいいという意見を持った人が多くいた．あえて，宣言されると余計なことが気になって嫌だからという理由が多かった．

しかし，これからの社会でこのような考え方は非常に危険になる．常に何か悪いことが起こった時の対策を十分に準備したり，悪いことが起こらないよう十分な対策を講じることを心がけることが重要なのである．そのことをただ理解しろといっても今までの習慣であったり，社会的環境が影響することなので，難しいと考えられる．そこで，実際に技術の先端にいる企業側が，消費者がきちんとした知識を持って行動できるよう何らかの対策を講じることが必要だと考える．このように，一般消費者が必要な意識改善をおこなえるかどうかというところの責任は企業にあると考える．

2.7.4 論点２－２まとめ

情報社会におけるセキュリティ対策の重要さ，既存の技術とその問題について検討することで，非技術的対策としてどのような対策が必要とされているかについての考察を論じた．情報セキュリティ分野の研究は，今まさに注目を集めている分野であり，認証方法，暗号方法等さまざまな角度からの研究がおこなわれ，日々進歩しているところである．認証技術に関しては，現在電子商取引市場が急速な発展を続けていることから政府サイドからの政策を含むさまざまな対策が検討されている．しかし，何かを守るための技術は同時にそれを破る技術も生まれることになり，それは常に悪意をもっているわけではないが，常に善意であるわけでもない．常に悪意をもっているわけではないのでそういった技術の開発自体を規制することはできないが，常に善意であるわけでもないので，何らかの規制をかけて悪用を防ぐ必要がある．

国境を越えた取引もあることから，政策として取り上げられるのは勿論重要なことではあるが，それと同じ位一人一人のセキュリティに対する意識を向上させることは重要である．

個人情報を必要とするサービスが増加したり，そういった取り扱いがユーザが意識することなくおこなわれるようになるにつれて，技術者サイドとしては，如何にユーザの手間をかけずに自然に情報の取り扱いをおこなうかという点に重点を置いて研究がされていくべきである．しかし，それは大前提として一人一人がセキュリティの重要さを把握し，それ相応の対処をしているという点が保証されているからこそ，検討されることができる新技術であるので，それを認識していない状態で進めていくのは極めて危険である．

社会全体としては，まず認証基盤を整え，個人情報管理に関して充分なセキュリティ対策をおこなうことが第一歩である．そして，一個人としては，一番身近にあるインターネットを利用する上でのセキュリティ対策をおこなうことが，自分たちの生活をサポートしてくれるような便利なシステムを生むための第一歩になるであろうと考える．

2.8　論点３－１：個人情報提供の判断基準

次に，非技術的対策をバックアップし，技術的対策を講じる上で検討されるべき概念を定義するための論点についてである．

論点１－１で，個人情報の自己管理システムについて論じた際，一般消費者が個人情報を必要とするような個人向けサービスを前にしたとき，何を判断基準として個人情報提供の有無を検討するかという点が不明確であるという問題を提起した．個人情報を自己管理するということは，自分で個人情報の提供に関して責任を持たなくてはならないということになる．一見，新たに与えられたすばらしい権利のように思えるが，きちんと理解した上で判断しないと，自分に責任があるので，何か起こった際に泣き寝入りということに成り兼ねないのである [23]．従って，何を基準に自分の個人情報の提供を検討するかということは，消費者にとってとても大きな問題となる．また，サービスを考える側としても，消費者が何を基準に判断するかを知ることは重要な要素となる．

本論点では，人の判断基準という要素を社会学的観点と，心理学的観点の２方向から検証することにした．

2.8.1　社会学的な判断基準

まず，社会学的に，人の決定とは何を基準におこなわれているのかということを考える．安田氏は「人を動かし，組織を動かしているのは関係（ネットワーク）の力である」[22] と論じている．確かに，人は，何かを決定する際，完全に自分だけの考えで，外部にで全く左右されずに判断を下すということはあり得ないのである．というのは，そもそも人の個人の人格という物自体がその人の周りの影響を受けて構成されているものだからである．完全に自分だけで自分の考えだけで何かを判断したと思っていても，自分がそういう考えを持つ人間になったのには，自分のネットワークが大きく関与しているのである．

ネットワークとは有効利用すれば，情報源になったり自分に取ってプラスに働くものだが，場合によっては自分の行動を制限したり，拘束したりすることもあり得るのである．

まず，何かの善し悪しを判断する際に,「常識的に考えて，こういう悪事は起こらないから安心して利用しよう」とか言う考えを持つことがあるが，そもそも ”常識 ”という概念こそ，自分の周りのネットワークによって構成されるものである．この場合，自分のいる環境における常識を念頭においているので,，非常に不安定で危険な意見である．問題は，自分の常識外のことをする人からどのように自分を守るかということなのである．

インターネット技術の普及に伴い，個人のネットワークというものの大きさも飛躍的に拡大化している．今までの人と人との関係によって編成されるネットワークのみならず，インターネットという莫大な情報量を持つグローバルなネットワークが各個人に与えられている．何かを調べようとする際，ネット上に莫大な量の情報があるという環境も自分のネットワークの一つである．そのような環境の一員である一消費者がどのような情報を持って個人を形成し，どのような要因で物事を判断しているかということを考える必要がある．自分の周りに IT 関連について詳しい人物がいる人といない人では，それに関する知識量が異なるので，異なる判断基準を持つことになるのである．

従って，社会学的な観点からこの問題を考えると，”関係 ”というものが大きく影響し，消費者側としては，知識を持った人とのネットワークが必要となり，サービスを考える側としてはこの要素から判断基準を導くという試みは，対処しきれなくなってしまうという問題に突き当たる．そこで，この概念を考慮した上で，次に，心理的に何が判断基準となるのかについて検証することにした．

2.8.2　心理学的な判断基準

では，人は何を基準に判断をしているのか．ここでの判断対象は勿論個人情報提供に関するものである．これに関しては自分の周りに話を聞いたり，周囲の協力を得てアンケートを実施したりすることで答えを導きだすことにした．実際には，どのような場合に個人情報を提供するかという問題に関しては，現状で考え易いように，買い物時のポイントカードのような物の作成に関連づけて検証した．

現状においても各店舗がそれぞれのポイントカードやカスタマーカードという物を用意して，買い物毎にポイントを貯めることによって特典が与えられるようなサービスを提供している．現状においては，毎回のように自分で必要な情報を記述している．一般的に要求される情報とは，住所・氏名・年齢・性別・電話番号である．これらは，個人情報の取り扱いを検討する際，一番始めに挙るような ”静的個人情報 ”である．現状では，これらの情報を特に気にせずに提供し過ぎなところがあるように感じる．

収集データの管理

現状では，買い物毎にポイントが貯まって，一定ポイント毎に特典があるという情報はわかっていても，自分の提供した個人情報がどのように利用されるかについての情報をきちんと理解している人は少ない．また，自分が記述して提供しているという方法から，その情報がデータベースで管理されているとか，ネットワーク上に情報が置かれているという事実気が付きにくいのではないか．しかし，実際には担当者が収集したデータをデータベースに入れて管理をしていると考えるのが普通である．

個人情報の自己管理をおこないつつ，さらに情報の提供に関しては手間をかけずにおこなうために，自動で取り扱いできるような環境を提供するという話になって初めて，消費者は自分の個人情報が必要以上に外部に流出していることに気が付き始めているのである．しかも，自己責任の基にである．

自己管理の重要性の認識

このような状況になった初めて，消費者は自分で自己管理をすることの大切さに気が付き始めている．こうなると，消費者は，世間が騒ぎ始めているからという理由もあるが，クオリティや自分の利便性のみならず安全性にも重点を置くことになる．実際に，アンケート結果からも今までカードを作成するかどうかという点に関して，特典や有効期限等しか気にせず作っていたものの，それによって自分の買い物履歴等がマーケティング用の情報として利用されているかもしれないと思ったら作りたくなくなったという意見が多くあった．

基本的に，自分がきちんと理解していない世界に関しては，初めは抵抗を持つという利用者が多く，実際に今まで自分が提供してきた情報においても同様の使い方がされていたとしても，実際に利用しますと宣言されると情報を提供したくなくなるとい

うケースが多くあった．しかし，知らなければいいという問題でもないので，消費者がきちんと理解した上で，何を基準に判断するかを検証すべきだと考える．

サービスを考える側としては，判断基準がサービスのクオリティ次第であれば，ユーザに合ったサービスを検討することが必要だし，そのサービスがユーザの生活にどれくらいの必要性をもたらすかということなら，ターゲットを決めてマーケティングを実行し，求められるサービスを検討する必要がある．

判断基準要素

一つ目として，行列が行列を呼ぶ心理と同様に考えると，自分より以前にこのサービスを受けた人がどのように感じたかというような評判情報を入手できたらこれも一つの判断基準となるのではないだろうかと考えた．そこで，論点１－２において，に評判情報を提供するようなシステムの構築を検証するとともに，評判情報が一般消費者に与える影響についてもリサーチした．

二つ目としては，利用頻度や特典のように自分にどれだけの利益があるかという点である．周りがどう思っていようとも，自分が頻繁に利用する店だったら個人情報を提供するだとか，自分への見返りが大きければ提供するといった考えである．個人情報を提供するにあたって安全性の確保という面では他者の意見が気になるが，実際に利用するかしないかという判断に関しては，自分主体に考える人が多い．

では，実際にアンケート結果がどのようになったか記す．

2.8.3　アンケート対象者

アンケート対象者としては，著者がどのような意図を持ってアンケートをおこなっているかということに関して特に情報を持っていない人を対象とした．従って，同じ研究室内の人は対象とせず，その親・兄弟，また，著者の家族の知人といった人を対象にした．こうすることで，どのような答えを想定してアンケートをおこなっているのかといったことを考えずに，自分を意見を応えてもらえると思ったからである．実際にアンケートを回収し，集計した結果，有効票となったのは表 2.1 の通りである．

	男性	女性	計
１０代	４	１２	１６
２０代	１４	１８	３２
３０代	２	１４	１６
４０代	０	６	６
５０代	１０	１２	２２
計	３０	６２	９２

表 2.1: アンケート対象

有効表として数えられなかった回答としては，全く買い物を自分でおこなわないため，ポイントカードなどについての知識がほとんどなかったものや，マーケティングや履歴確保のための個人情報収集に関して，理解していただけなかったものなどが存在する．

2.8.4　アンケート結果

アンケート結果を集計し，考察すると以下のことがいえる．数値的結果は，付録Bに添付する．

現在，店舗毎にポイントカードやカスタマーカードと呼ばれる物を提供する店が多数存在する．それらのカードは作成すると，買い物の購入金額毎にポイントが加算され，一定ポイントが貯まると何らかの商品がもらえたり，一定金額の金券代わりになったりするという特典を持っている．このような特典を消費者サイドに与える見返りはどのようになっているのかということを考えたことのある消費者はどのくらいいるのだろうか．カードを作成することによって，顧客の再来店を促すことによる収益アップが見返りだとしたら，個人情報は特に要求されないはずである．実際には，買い物履歴等からマーケティングがおこなわれていることが多いのではないかと考えられる．このような情報はカードを作る際に消費者に提供されているはずだが，それを認識していない消費者のほうが多い．

そこで，実際にポイントカード等を作成している人が，自分が提供している情報がどのように利用されているかを認識しているか，また，何を基準にカードを作成するか否かを決定しているかについてアンケートをおこなった．大半の場合，住所氏名年齢電話番号というまさに ”個人情報 ”と呼ばれる情報が収集されていることを消費者がどう感じているか，また，今まで気が付いていなかった利用方法に関して気が付いた今，それに関してどう思うかについても聞くことで，人の心理状態から判断がどのように変化するか等について考察を導きだしていく．

現在の環境においてポイントカードを作成するか

まず始めに，現在の状況で個人情報を提供してまでポイントカードを作成するといったことをおこなっているかについて検証した．現在，ポイントカード等を作成する際には，基本的に「○○ポイント貯めると特典があるので，お作りしますか？」程度のことを聞かれ,「はい」と応えると否応なしに住所氏名年齢電話番号と云った情報が要求される．現状で，このような状況でポイントカードを作成するかどうかを尋ねた結果，約８割の人が作ると回答した．作ると回答した中でも，年代・職業別に内訳を見ると，主婦層は九割以上，一方サラリーマン層は３割未満だった．これは，実際に買い物をする上で中心となっている人物が主婦であるからだと考えられる．また，高校生世代に関しては，男女問わず８割以上の人が作ると回答した．

しかし，カードは作成するものの，選択権があったら提供したくない情報として ”住所 ”という情報が挙っている．カードを作成して，実際には情報を提供している物の，もし提供しなくても同じサービスが受けられるなら ”住所 ”は提供したくないと考えている人が約４割も存在した．理由と尋ねたところ，住所という情報は一番個人を特定し易く，自分のプライバシ領域を侵害されるような気がするからという意見が多かった．

あえて在庫管理という利用用途を明確に伝えられたら

実際には，在庫管理や，マーケティングにも利用されていることが考えられる．従って，その旨を伝えられたらそれによってカードを作ろうと思っていた気持ちが変化するかどうかを検証した．それでも作るという人が多かったが，マーケティング等をさ

れると自分のところに余計なダイレクトメールがくるような気がするといった理由で作成を考え直すという意見もあった．初めの質問でカードを作成すると答えた人の中で，約３割の人が今回は作成しないというように意見を変えていた．

履歴が残ると気になるとか，余計なダイレクトメールが来る気がするという理由でカード作りを拒否する場合が大半だったが，在庫管理のための情報を利用するといわれても，それが自分にとってプラスになるとは思えないからという理由もあった．やはり，自分の情報を提供するからには，自分にとって明確な利点がないと提供する気にならないということのようである．さらに，個人情報提供の有無で一概にカードを作成するかしないかは決められず，その相手を自分が信頼しているかどうかということが関わってくるという意見もあった．

取得されたくない情報のタイプ

次に，買い物中に取得されたくないタイプの情報には，どのような情報があるかということに関してもアンケートをおこなった．勝手に取得されたくないかどうかを尋ねた情報の種類は以下の通りである．

- 入店時間
- 退店時間
- 購入品目
- 店内の移動経路
- 決算方法

この中で一番抵抗があったのは店内の移動経路であった．店内の移動経路に関してどのように情報を取得するかということに関する情報はあえて通知しない状態でアンケートをおこなった．これは，現状でユーザをサポートするサービスを構築する上で，利用が検討されている技術であるが，実際に消費者にそれに関する情報をきちんと提供しない状態で進められようとされていることから，それに関して消費者がどのように感じるかということを知りたかったからである．

何の前情報もなく，店内の移動経路に関する記録を取るといわれると，一般的には個人が特定され，監視されているような気になる．だからこそ，決算方法等の情報よりも移動情報というプライバシ情報のほうが取得されたくないと考える人が多かったのではないかと考えた．個人が特定できるかどうかは別として，常に見張られているような感じを持ちたくないという回答者が多かった．その割には，入退店時間を取得されることを嫌がる消費者は少なかったのには驚いた．自分が店内にどのくらいの時間居たかという情報は取得されてもかまわないが，常に見張られているのは嫌だということである．

しかし，実際には，同一店舗内の各エリア毎で出入りの時間を計測されていたらずっと監視されているのと同じような情報が取得されると考えられるが，情報を取得することに関して，継続的にずっと見張っているというような言い方とされると，それには抵抗を持つということのようである．

カード作成時に提供する情報について

また，カード作成時に提供する情報に関して，常に真の情報を提供するかどうかという点に関しては，自分としては，場合によってニックネームを利用したり，虚偽の情報を提供したりすることがあるだろうと予想していたが，そのように対処する消費者は思いのほか少ないことがわかった．アンケート結果からみると，八割以上の回答者がどんな場合においてもきちんとした個人情報を提供していることがわかった．

実際には，自分の身の回りの人から話を聞く限りでは，虚偽の情報を提供するかどうかの選択をおこなうという意見が聞かれたので，インターネット環境をよく利用していたり，ネットオークションを利用したりしている人は，ハンドルネームの存在等を理解しているため，提供する情報に関して，実情報を提供するか，多少偽るか選択をおこなうが，一般的に，虚偽の情報を提供するという意識自体があまりないのである．

抽象的な情報や，虚偽の情報，ニックネーム等を提供すると応えた回答者には，どのような場合にそのような情報を提供するかということを尋ねた．その結果，生年月日や電話番号・年収や仕事内容に関しては虚偽の情報を提供することが多いということがわかった．また，趣味嗜好と云った情報は現状では提供することで与えられる自分のメリットが明確でないことからマジメに回答しないという意見が多々あった．さらに，情報を管理している人が店頭に居る人であるような規模の小さな店では，どんな情報に関しても，実際にその場に居る自分と情報が結びついてしまうので本当の情報を提供しないという意見もあった．

以上のような結果から，自分は常に本当の自分の情報を提供しなくてはならないと思っていたり，情報と自分が簡単に結びついてしまうような環境においては，必要以上に抵抗感を持たれるということがわかった．現状のポイントカード作成の手順には，消費者に選択権を提供している物の，実際には，その選択権は作成を決定した時点で完全になくなってしまうように感じられているのが事実であると考えていいだろう．これでは，個人情報の自己管理は成立しないので，再検討が必要である．

また，実際に，個人情報取り扱いに関する情報を作成時に読んで十分に理解するよう努めているかどうかと言う問いに関しては，きちんと読むという人は明らかに少数だった．これは，はじめから、読んでも理解できないと思っていたり，自分に害がなければ構わないと思っていたりすることが原因のようである．

情報提供の判断基準

最後に，ポイントカードを作るかどうか聞かれた際，何を判断基準にしているかということを尋ねた．結果として以外だったことは，どのような個人情報を必要とされるかということに関しては，ほとんど気にされていなかったということである．回答として多かったのは次のような意見である．

- 利用頻度
- 特典内容
- 有効期限
- 店のブランドや評判
- クレジットカード機能を付けなくても利用可能かどうか

個人情報に関する意見が少なかったのには，個人情報が利用されるということに関してまだ理解が十分ではないからではないかとも考えられる．これは，この類のカードを作ることイコール一定の個人情報を提供する必要があるということで，一般に認識されてしまっているからではないかと考えられる.「個人情報を提供することで，特典が与えられます」という進め方ではなく,「特典が与えられますよ．では，個人情報を提供してください」という進め方なので，抵抗感が少なくなっていると考えられる．現状では，利用用途も限られていることから、このままの進め方で問題ないようだが，今後は，より多くの個人情報が必要とされることから，個人情報が利用されることを全面に押し出し，消費者がそれを理解した上で提供するような環境にしていくべきであると提言する．

2.8.5　論点３－１まとめ

一般消費者が，新しいサービスを前にしたときに何を判断基準にそのサービスのために個人情報を提供するか否かを判断するかについて，人が行為を決定する要素はそのネットワークに依るという社会学的観点と，個人の気持ち次第という心理学的観点の両側から検証した．社会学的観点からの見方については，文献を参考にし，心理学的観点からの見方については，アンケートや周りからの意見を基にまとめた．

社会学的観点からみたときの要点は確かに正しいと考えられ，実際に人が何かを判断する際には，その人がどういう人かという要素のみならず，その人の周りの関係がどうで，そのことが当事者にどのように影響を与えているかということが問題になる．実際に，今回のような場合においても，インターネット関係の仕事に就いたり，それに関する知識を持った人が周りにいる人といない人では，危険性の認識が異なったり，情報提供によるリスクの理解が異なったりするので，同じ判断を下していても，その自分に下した判断に対する責任の感じ方が異なっていたように感じられた．

実際，今後の環境構築を基に検討するには，全ての消費者がセキュリティに関する十分な知識を持っているということが前提となる．従って，個人情報の自己管理とは自分にどの程度の責任が発生するのか，自分は何を注意しなければならないのかということをきちんと把握した消費者が対象であるということを認識すべきである．

また，心理学的観点からみると，利用頻度や特典内容等，自分にとってどれほどの利益があるかという点が重要になってくることがわかった．個人情報を提供するということに重点を置いて考えると，店の規模や情報の管理方法が気になるところだが，基本的にはサービス自体をみて判断しているといえる．従って，判断基準としては，論点１－２で検証する評判が影響してくると考えられる．また，利用頻度が上位に上げられていることから，消費者にとって役立ち，かつ頻繁に利用しようと思えるようなサービスを提供することが必要である．さらに，クレジットカード機能を付けなくても利用可能かどうかという項目に関しては，クレジットカード機能を付けるにはそれ相応の個人情報を提供しなくてはならないから抵抗があるという意見もあったので，どんなサービスにどの程度の個人情報を要求するかということに関して，十分に検証することが必要である．

以上のことを考慮した上で，どのような情報を提供することで，どのような特典が得られるのかという情報をきちんと理解してもらえるような環境を整えることが必要であると提言する．

2.9　論点３－２：人間とサービスの関係

ユーザに適したサービス，ユーザが望むサービスを提供するために，人間とサービスの関係という要素を考えてみることも必要である．人は，コンピュータのことを人間として扱っているという説をとなえてる人もいる [24]．この説によれば，人は知らず知らずのうちにコンピュータを人として扱っているというのである．

2.9.1　人とコンピュータ

人とコンピュータの関係を考えるとき，まず人とメディアの関係を考えるとわかり易い．人は何かを理解するとき，自分が理解し易い形で理解しようとするのである．要するに，メディアにおける場合でも，実際に画面に映っている人は，仕事で役を演じているだけで，意見を考えたり，企画を考えたりしているのは裏方の人の役目であるのに，観ている人は，裏方を意識せず，自分が観ている人の意見であるかのように理解するということである．人はメディアを通して何かの情報を得たとき，実際にその情報を発している人からの情報としてとらえがちであるが，情報を提供しているのは裏方の人であって，その指示の基で演じている人間がいるということである．しかし，それをきちんと認識している人はそういないだろうと考えられる．

このメディアをコンピュータと置き換えても同じことが言えるのである．コンピュータで何らかの作業をおこなっているとき，実際にその作業をおこなっているのは，プログラムであって，コンピュータがそのような動作を実行するのは，プログラマがそう設定したからなのである．しかし，実際にはコンピュータが何かをしてくれたかのような錯覚に陥ってしまうのである．このことを，人がコンピュータを人として扱っていると言っているのである．例えば，人は TV 等をみているときも，すぐ自分がその世界に存在するかのようにのめり込んでしまいがちである．そのほうが理解し易いからである．何でもかんでも第三者的に観て，実際に出てくる情報をコントロールしている裏の人物の存在を理解し，話を進めていくのは極めて労力のいる作業なのである．

そこで，以上のことを考慮した上で，人とサービスについても検証していくことにする．

人とサービス

サービスとは何かということをまず始めに考える必要がある．ここで対象としているサービスは，ユーザの生活をサポートしてくれるようなアプリケーションのことである．消費者の趣味嗜好にあった店を通知してくれたり，生活に必要な情報を適切に通知してくれたりするようなサービスである．ということは，結局のところ，サービスとは，プログラムなのである．ユーザに合った環境を提供するようにプログラマが構築したシステムを，ユーザ情報を提供して稼働させることで，適切なサービスとして提供されるのである．

環境設定をできる限りユーザに手間をかけさずにおこなうようにプログラムされているため，自分が何もしてないのに，あたかもコンピュータが自分の趣味嗜好を勝手に理解して，適切なサービスを提供してくれているかのように思われる．しかし，実際は自分が初期段階で設定した情報を基に稼働しているだけなのである．

このような錯覚を覚えるということは，人はサービスを人として取り扱っていると言えるのではないだろうか．自分の生活をサポートしてくれる目に見えないロボット

と言ったところだろう．では，サービスを人として扱うとすると，人は自分を助けてくれる人に対してどのような反応をするのか．その人が間違ったことをしたらどの程度許し，どの程度で嫌いになるのだろうか．このことを理解することで，人とサービスのあるべき姿を探り，導きだしていく．

例えば，自分が信頼している人にだったら自分という人間の詳細な情報を提供し，その上で自分を助けてくれることを望むかもしれない．また，親しい相手なら多少のミスは許してくれるだろう．しかし，自分と相性が合わない相手だったら，たとえ自分に取ってプラスになってくれることをしてくれるとしても，それは，自分に取って余計おせっかいであって，受け入れないということがあり得る．人の好き嫌いは，基本的に規則性を見いだせるものではないので，そこから，どのようなサービスを作れば大勢の消費者に喜ばれのかということを判断するのは難しい．しかし，一つ分かることは，相手の機嫌を取るだけではだめだということである．

ロボットと友達の違い

しかし，ここが難しい点のような気もする．というのも，本当の友達であれば，自分の悪さを指摘してくれたり，嫌な役を買って出てくれたりしたら，後々それに感謝して，ということもあり得るが，友達のように接しているだけで，友達ではない．所詮ロボットという枠から抜け出さないとなると，自分の思い通り動いてくれなくなると，途端に機械としてみるようになるということも考えられる．人工知能学の進歩に伴い，ロボットが我々の生活をサポートするというような話も出てきているが，実際に映画等からもみれるように，所詮ロボットだからという考えが生まれがちである．筆者が想定する環境におけるサービスはロボットで考えられる生活サポートとは多少異なる点があるように思えるが，ロボットという形を取らないだけで，同様のサービスを提供するということも想定範囲内である．

問題は，人間が実際に何かを稼働させているプログラム自体をみるのではなく，表面上自分に関わっている媒体をみているという点に重点を置かなければならないという点である．ドラマ等を観ていて，自分の嫌いな役を演じている俳優に対して嫌悪を持つことと同様に，何らかの問題が発生し，ユーザに取って不利益が発生すると，裏で操って悪さをした人に対してではなく，自分に害を及ぼしたサービス自体に対して嫌悪感を持つのである．裏方を意識せず，自然に自分に適したサービスを与えてくれると錯覚をしているユーザにとっては，何か悪いことが起こったときも，そのサービスが悪事を起こしたと理解してしまう恐れがある．

2.9.2　論点３－２まとめ

人が，今後出現するであろう新たな形態のサービスに対してどのように取り扱うかということに関して論じた．人がメディアやコンピュータに対して，それを動かしている背後を意識せずに，そのものが自分に働きかけているかの如く扱うのは，相手を人として捉えているのと同様であると考えられる．

生活をサポートするようなサービスを検討するのであれば，特にその点に関して検証が必要である．新しく利用を考える際には，その対象に関する第三者の評判も影響するし，その影響とは全く別の指標で，自分に合っているかどうかという指標も重要になる．自分に合っているかどうかという点に関しては，サービスを検討する側とし

ては対処が難しいが，例えば個人情報の取り扱いに当たって利用者がどのような印象を持つかということに関しては，いい印象を持ってもらうために対処しようがある．

ユビキタスコンピューティング環境の目指す最終形として，サービスを提供するために，自分が何を提供して，どんな情報がどのように利用されるかということに関してユーザが特に意識することなく自然にその人に合ったサービスを提供するという点が上げられる．そのためには，消費者がサービスに対して自然に人と付き合うかのように取り扱ってもらえるというのはプラスであると考える．しかし，だからこそ一度嫌われたり，悪評をたてられると信頼の回復が非常に難しいということを前もって考慮するべきである．

2.10　論点３－３：信頼性

論点１－１，１－２で触れたように，プライバシの保護を実現するための個人情報の自己管理において，さまざまな箇所で信頼性という要素が重要な役割を果たしている．自分の個人情報を利用して，自分に適したサービスを提供してくれるという相手をどの程度信頼できるか，また全くの他人が評価した結果をどの程度信頼するかといった要素は，プライバシ保護を実現するシステムを構築する上でも十分に理解が必要な要素であるといえる．

人と新しい関係を築いていきたいサービスとしては，消費者がこの個人向けサービスに対して，どのような距離をもって接していくのかということを知ることは必要な要素の一つである．インターネットの普及はめまぐるしい早さで進行したが，それと同じように個人向けサービスも浸透していくのだろうか．この個人向けサービスは消費者からの信頼度の度合いが普及するかどうかに大きく関わってくるのである．

ここで，まず人がこの個人向けサービスをどのような対象として取り扱うだろうかという点に関して検討をすることから始める．一つ目は，現在普及しているインターネット技術の進化型としてみるというものである．もうひとつは，コンピュータの進化型として受け入れるというものである．論点３－２において，人はコンピュータを人として扱うと云う説を検証したので，これを基に考えると，サービスというもの自体を人として扱うということも考えられる．そこで，人が個人向けサービスに対して，インターネットの進化型として見るという見方と，コンピュータとして見るという見方の二つの見方から検証することにした．

2.10.1　インターネット技術の進化型として扱う場合

インターネット技術の普及により，人々の生活が変化してきていることは，疑い用のない事実である．実際，今までは用事があれば手紙を書くか，電話をするかという選択肢だったものが，E-mail というリアルタイムで伝達できるという選択肢が増え，これによって手紙のように遠方への連絡に時間がかかったり，途中で紛失したりと云う問題が改善されたと考えられる．また，電話も携帯電話という形態に変化したり，テレビ電話になることによって，話をしたいときにすぐ連絡できたり，直接顔を見て話が出来るということが可能になった．このような新しい技術は，初めはコスト問題があったり使い勝手が難しかったりで苦労することもあるが，多くの人が利用することによってコスト削減の実現になったり，一度使い方を理解したらその後が便利だったりということもあって次第に普及し，今やその技術なしでは考えられないという状況になっている人も少なくないであろうと考えられるほどにまで浸透した．

今後浸透するであろうと考えられる新しい技術は，このインターネット技術や，携帯電話の普及に伴って開発が進んできたものであるといえる．従って，固定電話が携帯電話と云う移動可能なものになったことのように，家やオフィスで PC を前にして利用していたインターネットが，わざわざ PC の前に行かなくても利用できる形態になったり，自分が自分の要求を打ち込まなくても，あたかもそうしたかのように必要なものが必要なときに自分の周りで必要な動きをしてくれるような環境になることが想定される．となると，この新しい形態のサービスをインターネット技術の進化型としてとらえる人が出てきてもおかしくないのではないかと考えられる．

そこで，インターネット技術や，それが提供するサービスに対する，人々の信頼感，思い等を検証することによって，新サービスに対する人々の信頼感や思いに関する考

察を導きだすことにした．

そもそも，インターネットがユーザに提供しているものはなんであろうか．インターネットは我々の生活に莫大な量の情報を提供している．また，自分が出向いていかなくても欲しいものが手に入るようなシステムを提供することによって，我々の生活をサポートしてくれていると考えられるだろう．では，そのようなシステムや情報に関してユーザはどの程度の信頼をもっているのだろうか．インターネットが提供する情報を，新聞やテレビのニュースが提供してくれる情報と同等の価値があるものとして扱っているのか，もしくは異なる信頼感を持っているのか．また，ネット技術により提供される我々の生活をサポートしてくれるようなシステムに関しては，絶大なる信頼をもって利用しているのか，そうでないのか．これらの点に注目して調査を行った．主な調査項目としては，

1. インターネットが提供する情報への信頼度
2. インターネット技術に対する信頼度（セキュリティ）
3. インターネット技術が提供する生活サポートシステムに関する信頼度

の三つが必要であると考えられる．

これらの要素に関しては，一部アンケートで取得し，自分の周囲から話を聞いたり，文献を集めたり，そしてやはりインターネット上にある情報を収集することによって検証することにした．

そのため，まず始めに自分がこれらの項目に対してどのように考えているかという点に関してだが，インターネットが提供してくれる情報には，信頼できるものも出来ないものもあると考えている．情報を信用するかしないかは自分次第だが，その際基準となるのはその情報の出所である．情報を提供している団体が，自分に取って信頼のおける団体であると判断できない以上はその情報を完全に信頼することはしないようにしている．信頼するかしないかに関しては，自分なりにその団体のホームページを見たりプライバシポリシを見たりすることによって判断している．また，個人情報を提供するという点に関しては，クレジットカード番号等，万が一にでも流出して悪用される可能性があると考えられる情報に関しては，絶大なる信頼を置ける相手としか取り扱わないことにしている．また，e-commerce 等，生活をサポートしてくれる技術に関しても，現状で信頼が置けるとされている相手として取引はおこなわないことにしている．

このように，自分も一消費者として，自分が新しいサービスに対してどのように感じているかということも調査資料の一つとして検証した．

上述した項目に関しては，アメリカの消費者団体 The Pew Internet and American Life Project や，Consumer WebWatch が，アメリカにおける人のインターネットへの信頼感に関してアンケートをおこなった結果が Trust and privacy online[25]，A Matter of Trust[26] に記されている．これらも情報も参考にして検証した．このアンケートの詳細については，関連研究で記した．

インターネットが提供する情報への信頼度

インターネットはさまざまな種類の情報を提供している．新聞や雑誌を出版している企業が，自社が所有しているホームページで同様の内容の記事を提供していることもあれば，ある分野の権威者がその専門分野に関する情報を一般公開しているサイト

もある．また，掲示板のように一つの議題に関して，さまざまな人が匿名で自分の意見や，勝手なことを記していることもあれば，個人が自分のホームページを用いて自分のために記している記事が，他人の目にとまりそれが情報となって他の人に影響を与えることも考えられる．

それぞれ信頼度は変わると考えられるが，一般的に匿名性が高い情報は，信憑性が低いと考えられている．情報の発信者に関するデータがきちんと公表されている場合，その情報に関して，責任を持っている人がいるということで，信憑性が高く受け取られるということが考えられる．一方，何らかの情報を発信しているにも関わらず，匿名性を保つことを選択すると，その情報を提供することに責任を持てないのではないかという疑いをかけられ，その情報自体の信憑性は低くなると考えられる．

インターネットにおける匿名性の確保は，インターネット利用上のユーザの権利であり，だからこそ提供できる情報というのもあるので，匿名性が悪いとは一概に言えないのが事実である．しかし，情報を信頼するかどうかということを考える際，情報発信者の特定が出来ているのといないのとでは大きな違いが生じてしまう．

実際には，人に聞きにくいことや，専門的な情報に関して，インターネットで検索できるということで利用している人も多く，医療情報等に関しては，インターネットでの情報がかなり高い信憑性をもっていることもわかった．しかし，これは日本における現状の問題が大きく影響しているのではないかと考えられる．というのは，医療情報に関してインターネット上の情報と直接医者から提供される情報のどちらの信憑性が高いかという点に関して，インターネット上の情報と応えた人のほうが若干多かったのである．現在，医療事故が多く発生しており，人々の医者や病院に対する信頼度が下がりつつある中，インターネット上の情報は自分が普段診察を受けられない偉い先生が提供している情報であったり，実際の人の体験談であったりするからそっちのほうが信憑性が高いと考えられている．しかし，アメリカにおいて同様の質問をおこなうと，インターネットにおける情報にも信憑性はあるが，やはり医師から直接提供された情報のほうが高い信憑性をもっていると考えている人のほうが遥かに多いのである．

これは，インターネットによって提供される情報と，そうでない実世界からの情報，それぞれの信憑性につながりがあると導けるのではないかと考える．結論としては，口コミ情報や噂のような種類の情報もあれば，専門的に正しいきちんとした情報もあるということを消費者が認識し始めているということになるのではないかと考える．筆者が調査した結果からみても，カテゴリによって，情報の信憑性が異なることがわかった．

インターネット技術に対する信頼度（セキュリティ）

セキュリティに関する信頼度は，セキュリティに対する知識がどの位あるかに大きく関わってくることがわかった．E-mail を利用するにしても，ネットサーフィンするにしても，ネットにつないでいる以上セキュリティ対策は必要不可欠なことなのだが，それに対する知識がないと，危険性もわからないから対策もおろそかになるという悪循環が発生してしまう．

インターネットに関した何らかの知識を持っている人は，それなりの対策を施した上で信頼できるとか，それでも信頼できない部分があるとかという判断をすることが出来る．しかし，知識の少ない人に取っては，たとえ，いわれた通りに何らかの対策をしたところで，自分がおこなった対策が何をどうするものかということがきちんと

わかっていない以上一概に信頼できるとかできないということを判断することは難しいのである．従って，セキュリティに対する信頼度はユーザのインターネット技術に関する知識の量や，周囲に詳しい人が居るかどうかということに関係するといえる．

生活サポートシステムに関する信頼度

最後に，生活をサポートしてくれるシステムに関してだが，これの前項目のセキュリティに関する考察を同じような考察が導きだせるのではないかと考えられる．e-commerce 等我々が今まで出向いておこなわなければならなかった買い物等を家で PC の前でクリックするだけでおこなえるようなサービスが提供されている今，消費者がそれに対してどのような信頼を寄せているのかということに対する信頼度である．

まず始めに，このようなシステムを利用するのは，主に，頻繁にインターネットを利用しているようなユーザであることを前提にするべきだろうと考えられる．そもそも初心者と考えられるようなユーザは，ネット上に個人情報を提供してサービスを受けるということはしないであろう．また，ちょっと慣れてくると，そんなサービスを利用してみるものの，要求されて個人情報を素直に提供して，それに対する危険性をあまり持ち合わせていないか，それなりに対策をしているから問題ないと考える人が多い．さらに，ベテランといわれるような人になると，まず個人情報を要求されたからといって素直に個人情報を提供しないことがわかった．ペンネームや虚偽の情報を提供しても受けられる範囲のサービスがあることを理解していたり，状況に応じて提供する情報の抽象度を変更したりといったことが出来るようになってくるのである．

筆者が想定する環境においては，このような事情に関して，消費者が理解した上でどのような反応をするかということが検証したいわけだから，危険性や，セキュリティの重要性を理解した上でユーザがどのように対応するかということを検証する．まず，そのようなシステムを利用する上でのセキュリティ対策を十分に施した上で，技術的に足りない面と，それを如何に補うかということを検討する．その上で，システムを利用することによって，自分に与えられる利益が，危険が伴うことよりも大きい場合，そのシステムを利用することを決定する．結果的に，彼らにとって，システムを利用することは必ずしもそれを信頼しているということにはならないと言う点に注目すべきであると考える．

インターネットの進化系として扱う場合のまとめ

以上のことから導きだせることとしては，新しい形態のサービスをインターネットの進化系として取り扱う人たちにとっては，インターネットに対する信頼等の持ち方をそのまま，新しいサービスに対する信頼の持ち方として考えることができ，それによると，大きく分けると

1. この分野についての知識があるのとないのとでは考え方に違いが生じる
2. サービスを受けることと，それを信頼していることとは違う

ということになる．この分野に関して何らかの知識を持っているからこそ懸念することもあれば，持っていないからこそ懸念することもあるのである．しかし，全体としていえることは，システムに関して最低限必要な知識を持って，講じるべき対策を施している場合は，多少のリスクがあってもサービスを受ける傾向にあるということだ

と考えられる．今後増加するであろう個人情報をネット上で取り扱うことを必要とするサービスに関しても，それがどのように利用され，どのように管理され，情報を提供することによって，自分にどのようなリスクが生じる恐れがあるのかという情報がきちんと消費者側に伝わった上でサービスを展開していくのであれば，十分に利用者は生まれるのではないかと考えられる．しかし，現状の状況から見ても，きちんと自体を把握してない上で利用を進めようとすると，必要以上の懸念を抱いたりすることが考えられ，そういったことはサービスの発展を妨げる結果を招く恐れがあるので十分に注意が必要である．

2.10.2　コンピュータの進化型として扱う場合

人間がコンピュータを人として扱っている [24] とすれば，人間が他人に対してどのように信頼性をもっているのかを検討することが，人が如何にサービスを信頼するかということにつながると考えられる．

サービスを人としてとらえたとき，その他人が，自分のために何らかのサービスを提供してくれると考えるか，あわよくば収集したデータを利用してその他人自身のために利用しようと思っているかもしれないと考えるか，この違いは個人情報を必要とするようなサービスが発展していくかどうかにも係ってくるのではないかと考えられる．

まず考えるべきは，信頼とは何かということになる．信頼することと，安心することは違うというところから考えなくてはならない．それぞれの定義をあやふやにすることは，このようなコンセプトに関して調査する上で非常に危険なので，それぞれの定義を記しておく．

信頼と安心

信頼とは，相手の人格や行動傾向の評価に基づく，相手の意図に対する期待のことであり，安心とは，相手の損得勘定に基づく相手の行動に対する期待のことである [27]．つまり，相手の行動によっては自分の身が危険にさらされる可能性がありながらも，相手がそのような行動をとらないであろうことを期待することを信頼と定義し，相手が自分を危険にさらすようなことをしたら相手にとっても危険であるからそんな行動はとらないであろうと期待することを安心と定義しているのである．自分の身に危険が及ぶ可能性がある状態を「社会的不確実性の存在する状態」と定義する．この社会的不確実性が存在する際，信頼が意味を持ち，存在しない場合は人は信頼しているのではなく安心しているのである．

ここで，気をつけるべきは，相手が自分のことを危険にさらすことは相手に取ってマイナスであるからそんな行動はとらないだろうという考えは，相手に取ってマイナスになるということで，社会的不確実性を打ち消していると考えなくてはならないということである．ということは，こういった考え方は信頼ではなく安心としてとらえられるということである．

では，実際に新しい形態のサービスに対する信頼感について検証する．まずは，この二つの関係でいつ信頼が発生し，いつ安全が発生するかについて論じる．

サービスにおける信頼・安心とは

サービスに対する考えとしては，提供した個人情報が悪用されていないかどうかという点に関して，悪用して，それが公表されたら企業に取って大ダメージだからこそそのような行動はとらないだろうということは，サービスに対する信頼ではなく，社会的不確実性を消した安心なのである．個人情報を提供することに関して，絶対的な信頼を寄せられないから，相手側の不利益を考慮した上で勝手に安心しようとしているのではないかと考えられる．このように社会的不確実性を打ち消した状態においては，信頼という要素は用いられない．

上述したような定義で安心と信頼を区別すると，信頼とは，社会的不確実性が存在する上で，相手が自分に不利になるような行動はとらないと期待することである．例えばサービス提供側が，消費者がマーケティング用に提供してくれる情報の中に偽りがないであろうと期待することは信頼という要素である．これは，別に偽りの情報を提供したところで，消費者側に害はないから偽りの情報を提供することも可能だが，マーケティングに協力して正しい情報を提供してくれるであろうことを期待している場合に起こる社会的不確実性が存在する上での状態だからである．

筆者が想定する環境では，情報選択の選択権は消費者にあり，サービス提供側は，ユーザが利用してくれることが発展への第一歩になると考えると，消費者から見た観点での社会的不確実性は消されて考えられる場合が多い．しかし，セキュリティの脆弱性等から発生する問題に関しては，現段階では，技術には限界があり，個人情報を提供する相手への安心は確立されても，技術的に確保しきれないセキュリティに対しては安心できない．しかし，収集した情報の管理は企業の役目だから，企業側が必要十分なセキュリティ対策を施すであろうということに関しては安心することが可能である．

信頼という意味では，悪事をおこなおうとする相手への信頼が必要なわけだが，その信頼は確保が難しいと考えられる．それは自分が信頼を寄せるべき相手がわからないという不確実性があるからである．これに関しては，大きく捉えて，社会全体としてこのような心配をしなくていい，信頼のおける社会となることを期待するしかない．また，国がそのような社会になるよう充分な法制度を施行するであろうことに対して信頼を持つのみである．

2.10.3　論点３－３まとめ

一般消費者が，今後増加するであろう個人向けサービスに関してどのように信頼関係を築いていくかという点に注目して論じた．この論点は，個人向けサービスを構築する上で何に気をつけて構築していくべきか，どのように浸透させていくかということを検証する上で必要不可欠な要件であると考えられる．

そのため，まずは人が自分の生活をサポートしてくれるというサービスに対して，どのような観点で接するかという点に注目をおき，現在普及しているインターネット技術の進化型として受け入れるか，コンピュータの進化型として受け入れるかの二つの見方から検証した．この二つの観点から検証することにした理由としては，サービスの特徴として，

- インターネット利用による情報の取り扱いが主流となる
- 人の生活をサポートするような形態になる

- インターネット・コンピュータ技術の普及により実現する

といった点があげられるためである．従って，今現在検討されている，一般消費者から個人情報の提供を要求することによって，そのユーザに適したサービスを提供するような環境を想定する場合，消費者が現在自分に慣れ親しみつつあるコンピュータもしくはインターネットの進化型としてとらえるであろうと仮定することは有用であると考える．

実際に，この二方向から検証を進めていった結果，インターネットの進化型として捉えると，それに関する知識の量に依って捉え方が異なり，コンピュータの進化型として捉えると，知識より人間味が影響してくるのではないかということがわかった．インターネット技術は，それに関する知識を持っている人と，持っていないで利用してる人とではセキュリティに対する考え方も異なるため，利用の仕方も異なってくる．コンピュータは自分が何らかの操作をすることによってそれなりの結果を返してくれるものであり，それを利用してインターネット技術を利用したりするのだが，コンピュータというもの自体としては自分が思ったことをしてくれる人のような存在として捉えられることが多いようである．

実際には，インターネットの進化型として捉える人と，コンピュータ進化型として捉える人の２タイプができるわけではなく，時と場合に寄ってそれら二つの要素が混ざってくるのではないかと考える．実際に，筆者が想定するような環境を構築するためには，それに関する知識のあるなしで大きな差が生まれるのは望ましくない．携帯電話が普及した際にも同様に知識のあるなしで差が生まれたが，今ではほぼ全体的に最低限の知識は共有されている．実際には，まだまだ高年齢者の方には利用が難しいとされているが，長い期間でみれば全体的に同様の知識を共有することは可能であると考えられる．従って，今後展開していくであろう個人向けサービスに関しても，全体的に必要不可欠な知識に関して共有することを可能とし，望ましい環境を構築するために，上手く展開していく必要があると考える．

また，安心・信頼に関する問題としては，社会的に人を信頼できる環境かどうかということが大きく関わってくる．現在，インターネット利用に関する問題が多発したり，個人情報取り扱い事業所からの個人情報流出問題等が取り上げられている．こういった問題が多発すると，個人向けサービスの発展に大きな悪影響をもたらしてしまうことが考えられる．個人情報取り扱いに関する社会的不確実性を完全に取り除き ”安心 ”を持つことは難しいので，現段階から個人情報取り扱い等に関する問題についてきちんと考えて物事を進めていくことによって，消費者からの ”信頼 ”を得ることが必要不可欠である．

2.11　論点４－１：個人情報の抽象化

最後のグループは，今後さらに技術が発展し，個人向けサービスが展開してていく上で，新たな問題として取り上げられるであろう論点についてである．

現状では，個人情報の提供とサービスのクオリティ向上はトレードオフの関係にあるという前提のもと議論が進められている．しかし，ここではあえて，果たして自分に適したサービスを受けるのに個人が特定できてしまうほどの詳細な個人情報が本当に必要不可欠とされるのかという問題を提起する．

例えば、三日前に来た女性と，今日今来ている女性と同一人物であるということがわかれば，その人にあったサービスを提供できるのであれば，完全に個人を特定できてしまうような個人情報を提供する必要はないのではないだろうか？個人情報とは，あくまでも何らかの方法で個人が特定できてしまうような情報のことを指すので，趣味嗜好，年齢等の情報を提供する必要があるとしても，それが個人情報として取り扱われなければならないような状況であるかを検討すると，必ずしもそうではない場合がある．論点１－１において，情報を詳細に定義するという段階で，抽象化というキーワードを出した．従って，本論点においては，個人情報の抽象化を用いることの可能性を考えていく．

2.11.1　同一人物の特定

一つの例を挙げて考えてみる．あるブランドショップで，顧客の購買履歴からその人に合ったセールスのお知らせをするサービスがあったとする．また，このサービスは購買履歴のみならずその客の年齢，性別等から最近の主流をもとにセールス情報等を提供することもしているとする．この場合，年齢・性別・連絡先という情報が必要となるが，連絡先をフリーのメールアドレス等にしておけば店側に自分の住所・氏名等といったような個人情報を提供する必要はないと考えられる．連絡先として住所を提供すると，まず間違いなく氏名も必要とされるが，メールアドレスは通常同一家族内でも異なったアドレスを持てるので，その情報のみで特定の個人に宛てた連絡を可能とするのである．

従って，例えば趣味嗜好情報を提供してもそれが自分の情報であるということを不特定多数の人に知られる危険がなければそもそも個人情報の保護ということを気にする必要はないのではないだろうかということである．

店側としても顧客管理をするのに個人情報を利用すると考えられるが，その人の住んでいる番地やアパートの部屋番号まで知る必要はあるのだろうか？それらの情報が必要になるのはダイレクトメールを送るような場合だけであろう．しかし，たいていの場合ダイレクトメールは封を開けられることなく捨てられることが多いのではないだろうか？また，封書で送られてくるような情報は今後減少していく．なぜなら，メールで配信したほうがリアルタイムに情報を配信できるからであり，今や携帯の普及に伴って，一人最低一個のメールアドレスを持つ環境になりつつあるからである．マーケティングするにしても２２歳の人と２３歳の人を別々にマーケティングすることはないのではないだろうか？分けるにしても２０代前半と後半といったくらいだろう．

以上のことを考慮すると，上記のような利用用途の場合，○○県△△市在住の二十代前半女性その１という情報で十分ではないだろうか？完全な個人情報でなくプライバシ情報という段階で済ませられるように，情報を抽象化して利用することを考えるべきである．そして同一人物が再度来店した際に同一人物だということを認識するた

めにユニークなIDを渡しておけば十分だと考える．その上で，購入履歴や，来店履歴等をマーケティングのために残すとしても，そのデータから簡単に一個人が特定されることはないので，情報提供する側としても気が楽なのではないだろうか．どんなときにどの程度の抽象化レベルを保てるかについては再検討すべき要件である．

問題があるとしたら，現実社会との融合によって個人が特定される可能性があるという点である．オンライン社会の中では，実際に相手に ”会う ”ということがないので，このような心配はないのだが，現実社会とのつながりがある状態においては，例えばコンピュータのデータベースにある情報だけでは，個人を特定できなくても，買い物の際関わった店員や，レジの人間の記憶に基づく情報とともに扱われたら簡単に個人が特定できてしまうのである．

人の記憶による個人特定

例えば，提供した個人情報が，自分の年齢，買い物履歴，性別だけだとしたら，マーケティングされた情報としても，○○代の男性は，△△のような商品を定期的に購入するという情報で，さらに同一人物を特定できるような何らかのIDが提供される．しかし，このプライバシ情報に店員からの個人情報が提供されるようになると，IDと一個人が特定され，一プライバシ情報がきちんとした個人情報になり，それが悪用されると完全なるプライバシの侵害になってしまう．

従って，完全なる個人情報を提供しなくてもいいような場合における，人のプライバシ情報と実世界の存在の情報が結びつかないような対処法を前もって検討しておくべきだと考える．実際に結びつかないような対処法といっても，人の記憶に関係することなので，技術的な解決策がとれるとは考えにくいので，ここは，非技術的な解決策で，情報の取り扱いに関する取り締まりを再検討すべきであると考える．

また，実世界において，どこかに出向いて受けるサービスに関しては，自分にそのつもりがなくても個人が特定されてしまう場合があることを認識すべきである．実際に，コンビニなどで働く人は，長期間働くと，常連の客や，その客が好むタバコなどの情報を自然に把握できてしまうという話を聞いた．このような問題は，新しい技術が入る入らない以前の問題で現に発生しているものの，それが悪用されていないから見過ごされているだけなのである．しかし，悪いことが自分に降り掛からなければOKという状況で済まされる時代は終わりつつあることを認識すべきである．また，これは新環境における特別なことではないが，仕事場で入したどんな情報もそれは仕事中に入手した情報であるので，社外秘にするべきであることを，立場がバイトであろうが，社員であろうが関係なく，情報化社会の一員としてきちんと認識すべきである．

次に，電子決算の問題について論じる．この場合は，抽象化によって匿名性と保つことが問題となる，きちんとした個人特定が必要とされるという例である．この問題に関しては，既存の法案を基に，新たな技術的対策を提案する．

2.11.2 決算

実際にきちんとした個人情報が求められる例としては電子決算を挙げる．ここで，「個人情報が求められる例」としたが，実際には,「個人を特定する必要がある例」と言

い換えたほうが適している．お金が関わったり，取引をおこなったりして，双方に責任がかかる電子決算などの場合にはきちんと個人を特定できる必要がある．決算をおこなう際の，個人認証に関しては，未だ原始的な手法が取られているというのが現状である．今回対象としている環境は，個人情報をネット上で取り扱う場合ということなので，決算等もキャッシュレスでおこなわれるような環境を想定している．そこで，現段階としては，インターネットショッピング等で話題の電子決算を例に検証した．

問題は，現在の電子商取引における決算はクレジットカードや銀行振り込み，引き落とし等でおこなわれているものの，それぞれ認証方法に問題があったり，取引をおこなうどちらかにリスクが伴っているという点である．クレジットカード決算の場合，カード番号と有効期限がわかれば大抵の場合取引が成立してしまう．しかし，それは，カードを所有しているということが，カードの所有者であるということを証明していることになっているからであって，本当に今カードを所有している人が，そのカードの所有者かという点においては考慮されていない．そのため，実際に現金を引き落とす段階になってカード所有者からそのような覚えがないと訴えを起こされる危険性を伴っている．また，このような現象は，カードを盗まれたから起こるだけではなく，本当は自分が取引をしているのにそれを否認しているだけという可能性もある．このような問題を残したまま電子商取引で利用するのは非常に危険である．カードによる決算は，国境を越えた決算にも利用可能なため，有効的な手段ではあるが，本人の認証方法に問題がある．また，銀行の引き落としは国境を越えた決算には利用できないし，振込は，消費者側にきちんと商品が届けられるかという不安が残る．

日本特有の方法としては，ネットで購入したものを，コンビニで支払いと同時に受けとるという方法がある．これは，双方に危険性がおよぶ恐れはあまりないとされているが，極めて原始的な方法である．

以上のことを考慮した上で，キャッシュレスな環境が構築された場合について検証してみた．まず，キャッシュレスで取引をおこなう場合，消費者はカード番号を取引相手に渡す必要が出てくる．しかし，この情報は個人を特定してしまうような ”個人情報 ”になるのだろうか．クレジットカード番号を渡すということが，完全なる個人情報の提供になると言われているのは，クレジットカード番号という情報を利用して，カード会社の所有している顧客情報と照会することで，その個人を特定するというようなことが可能となるからである．

しかし，カード会社の所有する個人情報は，基本的に外部に流出してはならないものであり，従って，カード番号を教えることと ”個人情報 ”を提供することはイコールにはならないはずである．カード作成時に，カード会社を信頼した上で，利用者は自分の個人情報等を提供しているのだから，信頼の基提供された情報は，カード会社の管理のもと保管されなければならないことになる．この信頼を裏切ることは，論点１－１で論じたように個人情報保護法違反ということになる．

実際には，カード番号と共に，自分がその持ち主であることを証明するための何らかの個人情報を提供するから，その番号が個人情報と言われる種類の情報になってしまうのである．では，この認証の部分に新たな技術的対策を講じることで，個人情報を提供することを回避できないだろうか．そこで，カード番号を個人情報のつながりを検討した上で，次のようなフレームワークを提案する．

カード番号と個人情報

クレジットカードを作成する際には，クレジットカード会社との取引上，きちんとした個人情報が必要とされ，その情報と個人を結びつけるのがカード番号である．

では，実際にカードを利用する際の問題について検討する．その場に持ち主がいる場合，直筆のサインが本人認証となっている．しかし，そのサインが本物かどうかはカードの裏面に書かれたサインとの比較であり，大抵の場合そのサインはたいしてきちんと確認はされておらず，また，似せて書くこともそれほど難しいことではないというのが現状である．そう考えると，クレジットカード利用における認証の問題は現状で既に存在しているのである．しかし，インターネットという新しい基盤におけるプライバシ関連の問題が騒がれる中，クレジットカードにおける問題も新たに誕生したかのように取り上げられるようになった．

では，どのように解決すべきだろうか．クレジットカード番号から連結される個人情報に関しては，カード会社が守るべき個人情報であるので，これが流出することがあるとしたらそれはその会社のセキュリティに問題があるということになる．従って，それはセキュリティの問題として論点２－２で検討した．ここで考えるべき問題は，カード番号の情報を提供した人と，カード所有者が同一人物であるかどうかの認証という点にある．この認証のために，取引相手の自分の個人情報を提供するということになると，”個人情報 ”の提供が必要とされるが，本当に個人情報提供以外の方法はないのだろうか．クレジットカード番号所有者と，カード所有者が同一人物かどうかという点に関する認証はカード会社に委託することで，個人情報提供を回避することができるのではないかと考えた．

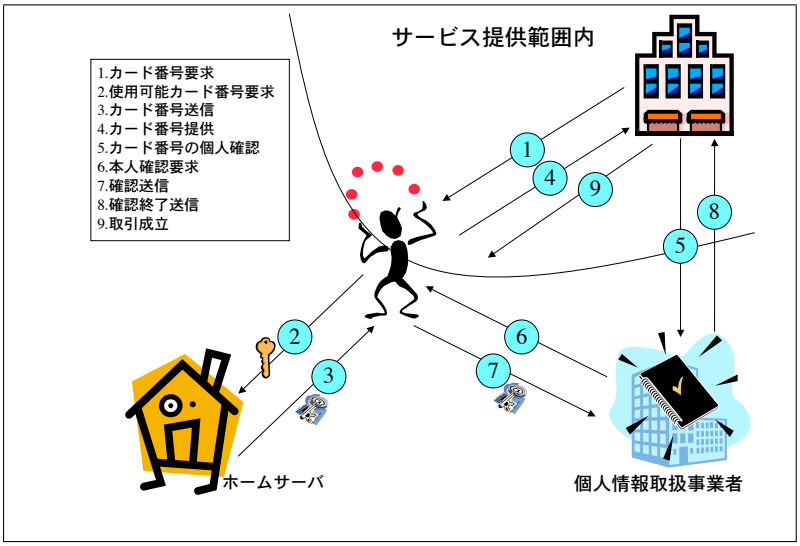

図 2.3: 認証システム

取引における経路としては，商品購入もしくはサービスを受ける際に，消費者はカード番号を取引相手は渡す．その情報をサービス提供側はカード会社に確認を取る．カード会社はカード番号から所有者を特定し，確認を取る．確認がとれたらその旨をサービス提供者に返す．この一連の流れを円滑におこなうことが出来るようなシステムの構築が出来たら電子決算における認証の問題は解決する上に，サービス提供側には個人情報を提供せずに決算をおこなうことが可能となる．勿論問題は，カード会社が如

何に認証をおこなうかという点である．

決算用認証

では，カード会社側としてはどのように認証をおこなうことが望まれるだろうか．このシステムを検討するには，ネット上で情報を取り扱うことに関して十分なセキュリティが確保されているということが大前提となるが，一度に全てのことを解決することは出来ないので，今後想定されるであろう環境においては，これらの前提がきちんと確保されるであろうことを期待して話を進めていくことにする．

カード会社としてはカード作成時に消費者の個人情報は把握しているので，カード利用の報告が入った時点でその情報を用いて当人に確認を取ることが出来るのではないかと考える．毎回電話のような方法で確認をとるのは非現実的なので，現在，利用の普及を進めている電子証明書を何らかの方法で利用することにより認証することがいいのではないかと考える．認証における流れは、図 2.3 に示した。

ここで考えられる問題としては，カード番号というユニークな ID を利用すると，同じサービスを受ける際，履歴を残したくなくても履歴が残ってしまったり，同系列のサービスであったり，万が一何らかの形で情報が流出したときに，その番号からさまざまなプライバシ情報が集まってしまう可能性があることである．そこで，カード番号というユニークな情報を提供するのではなく，カード番号につながるワンタイム ID[9]のようなものを使うことを提案する．

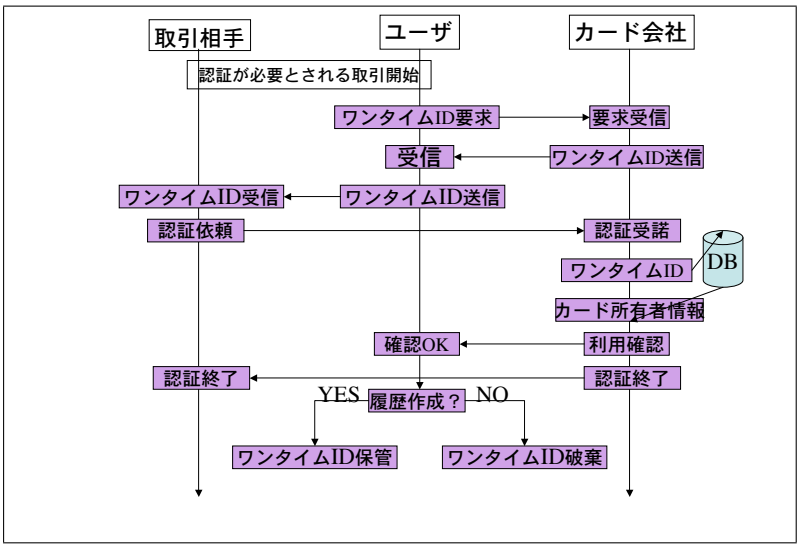

図 2.4: ワンタイム ID

同じサービスで履歴を残したいときは，同じ ID を利用し，そうでない場合には ID を発行してもらうようにすることで，初めに記述した問題は解決される．ワンタイム ID 取得のための流れは図 2.4 に示す通りである。実際に履歴に残っていないサービス相手にカードを利用とした際，カード会社にワンタイム ID の発行を求め，利用する．その後，同一のサービス内で履歴を残したい場合はそのままその ID を保管し，再利用する．もう二度と同じサービスを利用しないと判断したり，次に同じサービスを利

[9]ワンタイム ID：一度しか使われない ID のこと

用する際もまた新規として利用したいと考えた場合にはその ID を破棄し，再度新しい ID を取得すれば全くの別人として同じサービスを受けることが出来るのである．

2.11.3　論点４－１まとめ

消費者が自分に適したサービスを受けたり，取引の円滑性を追求する上で，個人情報を要求されるという状況において，きちんと個人が特定できてしまうような ”個人情報 ”を渡さないといけないような状況はあるのだろうかという点について論じた．個人情報とは，個人が特定されるような情報であるが，現状で求められているものは同一性が求められれば十分であったり，何らかの方法で連絡が取れれば十分であったりといった状況が多く存在するので，きちんとした個人情報が必要とされる場合はそれほどなく，情報の抽象化を可能にすることで匿名性を保てるのではないだろうかという疑問を持った．

現状では，ダイレクトメールが頻繁に使われることから住所氏名といった個人情報が必要とされるが，E-mail や携帯メールの普及に伴い，これらの情報も必要ないものとなりつつある．となると，E-mail は個人に唯一のものであるからその情報で同一性を確保できれば十分ではないかと考える．基本的に，E-mail も個人につながる情報であるから個人情報として扱われるべきではあるが，この情報だけで実在する人物と結びつけるということは，合法的には出来ないはずである．また，E-mai 情報は，住所氏名等の情報を提供するより簡単に提供し易いのではないだろうか．この情報で，同一性が保たれるのであれば，趣味嗜好，買い物履歴等についても，簡単に個人と結びつかないことから提供し易いのである．

このように，確実に実在する人物と結びつかない情報であっても，同一性を保証できる情報であれば十分にサービスの質を保てる場合がある．つまり，場合によっては個人情報となりうるプライバシ情報であっても，消費者が提供し易い環境を提供することで，余計な懸念を持たせなくてすむのである．自分に合ったサービスが提供されたり，めんどくさい手続きが必要なくなるためとはいえ，何でもかんでも住所氏名といった情報とともに提供を求められるのではなく，本当に必要な抽象レベルを定め，その情報のみを要求することで，消費者にとって抵抗なく情報提供が出来るような環境を整えることができる．

また，論点２－１で提起したように，日本におけるプライバシの考え方は，まだまだ浅く，情報の取り扱いに関して重要性・危険性の認識が薄いと考えられるので，個人情報の抽象化に関してめんどくさいと考えられがちだが，こうすることで，匿名性を保つことが以下に重要であるかということも認識すべきである。

その上で，実際に取引をおこなう場合等，個人を特定する必要がある際には，自分が絶大なる信頼を寄せている第三者を介すことで，低信頼の相手に個人情報を提供しなくても認証をおこなえ，それによって，高信頼の相手としかできないと考えられていた電子決算等の新技術を汎用的に利用できるようにする仕組みを提案した．

2.12　論点４－２：自動的に取得されてしまう情報

最後に，自動的に取得されてしまう情報に関して論じる．

機器の小型化等に伴い，さまざまな情報が消費者に知らされることなく収集されることが可能となった．このような環境においては，その新技術の使い方を制限し，消費者からの理解を得た上で利用を開始するようにしないと，悪用され始めたら大変な事態を引き起こしかねない．また，それはせっかく解決された新技術を全く実用性の持てない技術として壊す恐れがあることなので，きちんとした知識が必要だと考える．

技術の進歩によるデバイスの小型化は，消費者のためのサービスでのみ利用されるのではなく，店側としてのコスト削減や，防犯のためにも有効利用されている．例えば，小型タグによる万引き防止や，在庫管理等である．このようなタグの持つデータは主に商品そのもののデータであり，従って個人情報とは関係ないと思われガチである．しかし，そのタグが持つ情報の利用の仕方によってはプライバシ情報になり得るのである．そこで，このように，消費者自身が提供するわけではない情報で，状況に応じて個人情報になってしまう可能性を秘めたような情報の取り扱いはどのようにすべきかという問題について考察をおこなう．

例えば，位置情報についてである．位置情報というのは，その人が今どこに居るかという情報だったり，どこを通ったという情報だったりする．このような情報は，自分が明示的に情報を発信していないのにも関わらず，取得されてしまうことが頻繁に起こりうる．このように，情報が勝手に取得される状況は，大きく分けて２つあると考える．一つは，情報を取得することを目的としている防犯等に使われるケースであり，もう一つは，情報を取得することを目的とはしていない防犯や商品管理のためのデータが悪用されるケースである．まずは，これらのケースに関して，タグを利用する場合について論じることとする．

2.12.1　防犯に利用される場合

最近目にするようになったのは，CD 等簡単に万引きできてしまうような商品や，小型で高価な商品に取り付けられているタグである．そのタグが外されずに店舗から出ようとすると警告音が鳴るというものである．これらのタグは，防犯の目的にのみ付けられているものなので，会計と同時に取り外されるため消費者側に害はない．また，犯罪を抑制する目的もあるので，タグが付いていることが明示的に分かるようになっている．

しかし，この手法だと，このセンサーを外してしまえば容易く外に出れてしまうので，防犯用のタグが商品製造時に埋め込まれ，一般消費者からは取り外しができないように工夫される流れができ始めている．となると，今度懸念されるのは，そのタグを悪用する者の存在である．

タグ情報はタグリーダが近くにあるとそこで情報が読み込まれる．タグにはその商品の情報しかなかったとしても，タグが読み込まれた位置から，その商品を持った人の位置情報がわかってしまうのである．このことから，ある特定の商品を購入した人を知っている第三者が，商品の読まれる経路をたどって，その人を追跡することが可能となってしまう．

対策案としては，アルミ箔でタグをカバーすることによる電波妨害や，スキャン機器への情報伝送をブロックすることによるデータ収集を妨害する機能を持った blocker タグ等 [18] の開発が進められている．この blocker による対策のように，きちんとし

た対策案を出してから市場に広めないと，タグを利用する事自体に対し消費者団体から非難を浴びることになり，この技術を使うことができなくなってしまう恐れがあるため，十分な注意が必要である．

2.12.2　在庫管理等に利用される場合

次に，在庫管理等に利用される場合についてである．RFID のような小型タグの低コスト化や新技術の発展に伴い，商品の在庫管理やマーケティング等にタグが利用されることが検討され始めている．

しかし，同時に消費者達がその技術を知り始めることによって，プライバシ侵害の懸念を持ち始めている．タグに多くの情報を持たせることができるようになると，商品情報とともに，購入日時，購入者の抽象的情報等の情報も持たせることが可能となる．さらに，商品の品質管理という用途も兼ねている場合，その商品がどのようなルートを通って，どういう経路で店頭に並ぶことになったかという情報を持つこともできる．このようにすると，その商品特有の情報を持ち合わせることになり，簡単にあるものを特定できるだけの情報を提供することの可能になる．そのような情報を持ったタグが店舗外に出て，関係のない第三者によって情報を引き出されると，その商品をトレースすることで購入者の移動履歴まで漏えいしてしまう恐れがある．

このように，消費者の行動履歴が漏えいしてしまうことは，ロケーションプライバシ[10]の侵害として注目を浴びている．会計時にタグを外して再利用するという方法も検討されているが，小さいタグを消費者にわからないところに付けておくのが目的となる防犯用途もあるので，その方法をとることが最善策であるとは一概に言えないのが現状である．

2.12.3　その他の場合

上述では，商品に付けられたタグに関して論じたが，他にも自分の知らないところでプライバシが侵害されることが可能な例がある．例えば，最近の映画でもあった例だが，小型カメラによる防犯目的の撮影情報がリアルタイムにどこかで一括管理され，監視されているといったようなシステムが現実に起こらないとは限らないのである．この場合，システムが必要としている情報の対象者は一般消費者の情報である．利用用途が防犯とはいえ，自分がいつどこで誰と何をしていたのかという情報がデータとして記録されてしまうのである．犯罪を未然に防ぐためであるとか，治安を維持するためという目的であっても，そのデータをリアルタイムで管理するには，情報はネット上を飛び交うことになり，その情報を違法利用することも可能なのである．

例えば，その映画の例が実現したとする．カメラを設置した位置全てに警官が立っているとしたら同じ効果が出るわけだから我々一般人としては文句は言えないかもしれない．しかし，そこで取得されるデータは映像データのみならず会話まで取得されてしまう．しかも，所々で取得されているデータを収集して解析することで，自分が歩いている経路，誰と歩いているか，等，どこで何をしているかという情報が鮮明に取得され，記録されてしまうのである．これらの情報はきちんとした目的でのみ正しく利用されることが保証されるのであれば，防犯としていいかもしれない．しかし，

[10] ロケーションプライバシ：位置情報が取得されることによって，個人のプライバシが侵害されるという話の際に頻繁に利用される単語

このような技術が実際に使われるようになれば，データをハッキングしようとする人は確実に現れる．映像情報等は，自分が拒否したくても映らないようにすることは不可能である．そのような状況における対処法もきちんと検討すべきだと考える．

2.12.4　技術的対策

この問題における技術的対策の一つは，論点２－２で述べたセキュリティ対策である．情報が取得されることを拒むことができないのであれば，収集された情報が悪用されないような対策を望むことしかできないのである．映像で残る情報は，名前といったような個人情報が漏えいするより抵抗のある情報である．従って，これらのデータが取得された直後に暗号化され，映像的データではない形で通信がおこなわれることによって，第三者が介入しても簡単に復元できないようにするといったような対策が望まれる．

また，タグ等情報を発信してしまう技術に関しては，機能を無効化する技術の開発や，タグに埋め込まれたデータ自体の解読を容易におこなえないように暗号化技術を取り入れる等といったような対策が必要とされる．

2.12.5　非技術的対策

さらに，非技術的対策としては，これら，ユーザの意図とは別の情報を発信してしまうようなタグ等の技術について，十分に消費者理解を求めることが重要だと考える．非接触型タグは，タグリーダがあれば勝手にそれに対してデータを送信することができるという点が特徴になっている．これを有効利用することによって，コスト削減になったりすることから全体的に商品コストも下がって消費者にとってプラスになるという利点も持ち合わせる．しかし，一方で，情報が送られるべきでない所にまで情報が送信されてしまう恐れがあるという危険性を持ち合わせている．

消費者に新しい技術として紹介する際，こういった利点ばかりに焦点を置くのではなく，それに伴ってどのような問題が発生する恐れがあって，現状でどのように対策を施しているかといったことも同様に公表するべきである．利点に焦点を置いて技術を普及させて，後から問題が発覚した時に騒ぐのでは，せっかくの技術を十分にいかせない状況を作りかねない．従って，技術的対策で提案したような，タグの無効化対策や，情報の暗号化対策を施してる旨も十分に公表するべきである．

このように，公表した上で，新しい技術を取り入れるのであれば，自分の知らない所で勝手に何か情報が漏えいしているという余計な抵抗感を与えなくて済むことになるのである．

2.12.6　試験的に導入されている例

では，実際に特定の人を認識するのに利用される例に付いて紹介する．一つは，米オハイオ州の保護警務局が発表した例 [19] で，もう一つはフロリダのあるテーマパークが親に子供の居場所を確認する手段として提供している例 [20] である．

刑務所での使用例

米オハイオ州では，全受刑者が腕時計サイズの送信機を着用し，刑務所側でこの信号を追跡し受刑者の居所を把握するようにしている．このシステムでは，送信機を無理矢理とろうとすればそれを察知してコンピュータに警告を送れるようになっている．

刑務所という空間は，自由が制限されている場所であって，そのためこのようなシステムがあっても問題とはされないが，その他の場所でこのシステムを利用するのは人権無視ということになり，取り入れは難しい．

しかし，例えば親の監視下にある子供が付けていることによって，迷子になったりすることを防ぐことも可能になることから，一定の状況下で利用することは有効かもしれないと考える．実際に，強制的な監視下ではない状況で利用しているのが，次のテーマパークにおける例である．

テーマパークでの使用例

フロリダのテーマパークにおける使用例は，来場者全員に RFID タグ付きリストバンドを配ることで，位置特定をできるようにしている．埋め込まれたタグは，１４万平方フィートの園内各所に設置された読み取り機器に位置情報を無線で送信できるようになっている．来場者は，SafeTzone Real-Time Location System という名称のシステムに接続されたタッチスクリーン式の端末を用いて，仲間の居場所を確認できるというシステムである．このシステムは，園内に居る間だけの話であり，また，混雑している場所できちんと仲間の場所を特定できるということで，好意的に利用されている．また，同じような状況で同システムを取り入れているテーマパークは他にも存在するという．

先ほどの例と同様，限られた範囲内での有効利用は今後もさらに必要とされ，それに伴う技術の発展は望まれるところである．利用の進め方としては，監視と云うキーワードが使われてしまうような方法ではなく，あくまでもサポートというキーワードが使われるといいのではないだろうか．公表の仕方，利用の仕方によっては，その新しい技術を用いることによって，自分達の生活が監視され，プライバシが侵害されるという懸念をもたれてしまうが，逆に方法を検討すれば，自分達の生活をサポートするサービスと認識され，広く認められるものとなり得る．

最後に，実際にこの新しい技術の発展に伴って検討された，非技術的対策を紹介する．日本では，今年の三月に経済産業省から「電子タグに関するプライバシ保護ガイドライン」[21] が発表された．これは，商品等の情報を記録した IC チップを付けて，電波や磁器で情報を読み取るもので，消費者に商品の出所情報を提供するための商品追跡管理や商品の低価格での提供を可能とする流通の効率化・効率的在庫管理に役立つとして期待されている電子タグに対し，遠隔から情報を読み取れるという固有の特性が引き起こす問題を関係事業者団体がきちんと考慮した上で，開発を進めるようにという目的で作成されたガイドラインである．このガイドラインには，上述したように，問題性を理解し，その問題を以下に解決するかを検討した上で，新しい技術を公表するべきであることが定義されている．詳細は，付録 G に記述する．

2.12.7　論点４－２まとめ

自分で提供の可否を判断することができない情報について，その情報が取得されることによって，どのような問題が発生し，それに対し，どう対処すべきかということに関して，例を挙げて紹介した．センサー技術の発展に伴い，さまざまな情報収集が可能となってきた．しかし，これらの技術が更なる発展を遂げ，もっと市場に出回るようになる前に，考えなければならない点が多々ある．それは，新しい技術を利用して何ができるかという技術的なことよりも，新しい技術をどのように利用することがベストなのかという非技術的概念を検討することである．この問題についてきちんとした議論がされていないと，この新技術は消費者の生活を窮屈にするものになってしまう．

RFID のようなセンサ技術の問題は，タグを所有している者が明示的に何か行動を起こさなくてもそのタグに含まれる情報を提供できるという利点をついた攻撃によって，第三者にその情報を盗まれる可能性があるという点である．例えば商品情報だったとすると，その情報だけでは，個人を特定できるわけでもなく問題はないと思われがちだが，その商品を追跡することが可能になってしまうので，○○という商品を持った人が今どこに居るというプライバシ情報が流出してしまうことになる．また，その情報と何らかの他の情報を組み合わせると個人を特定することも可能になってしまう．このようなロケーションプライバシの問題は RFID 技術を市場に広げるためには解決しなければならない問題の一つである．

解決策としては，いくつかの方法が検討されているが，実際に消費者を完全に納得させるような解決策が出ていないのが現状である．そのような中で，商品管理のためとはいえ全ての商品に製造段階でタグを埋め込むといったような話題が持ち上がれば，消費者団体から反対の声が上がるのは当然である．従ってこの件に関しても，さまざまな視点から問題解決のための対策を検討すべきなのである．

本論点における対策としては，技術的対策は，論点２－２で紹介したセキュリティ対策の他に，新しい技術であるタグを埋め込むことによって，消費者に商品情報を提供できるという利点を強調できるよう，その情報が，消費者のロケーションプライバシを侵害することなく提供されるような対策が必要とされる．blocker による電波傍受のように，やたらな所に情報が流出しないような対策が必要とされるが，情報が必要とされる箇所もあるので，いつ電波傍受するのかとか，どのようにおこなうのかといったようなことを考えると，消費者が操作しなくてはならない所も発生してくると考えられ，それはそれでまた手間のかかることなので，実際に技術的解決策を検討するのみならず，それを実際に実行する際の手順も検討した上で最善の策を検討すべきである．

また，非技術的対策としても，セキュリティ対策の他に，電子タグ利用におけるガイドラインのように，新しい技術を取り入れる上で，どのような問題点が発生する可能性があるのかということをまず初めに検討し，対策を立て，それを公表した上で利用するという手順で広めていくべきであると考える．

このように手順を踏んで広めていくことで，RFID 技術が人々の生活を監視するものではなく，サポートするものだという認識を持ってもらえ，技術の発展につながると考える．

2.13 Penatesの評価

では，今までの全ての考察を基に，論点１－１で紹介したPenatesをプライバシ保護実現するためのシステムとして完成させるために何ができていて何ができていないのかの評価をおこなう．

結果は，各グループ毎に，どのような問題があって，それをどのように解決に導いていくかということを表として表すとともに，詳細を説明した．

2.13.1 グループ１

技術的対策が必要とされているグループ１（表： 2.2）については，個人情報の自己管理という分野がまさにPenatesが構築された目的を表しているので，技術的対策としては実装済みなところがほとんどである．しかし，実際に個人情報の提供の可否を判断するという段階における消費者の立場に立って見方をすると，判断基準が設けられていないことは致命的な要素であると考えられる．判断基準に関しては，以降のグループで詳細を論じているように，きちんと考察を提供し，必要とされる環境も提案してあるので，提案済みとした．

Penates	問題提起	技術的対策	非技術的対策	完成度 ・評価
個人情報の自己管理	個人情報の利用用途を如何に把握するかが不明確	一般消費者に半強制的に利用用途を通知	個人情報保護法	実装済み
	手動での個人情報提供は円滑な取引の妨げになる	できる限り自動で個人情報が取り扱えるようなシステムを構築	—	実装済み
	自己管理のための判断基準がない	評判システムの提供	判断基準の提供	研究・考察済み
評判システム	実体験に基づいた情報提供	オークション用の既存の評判システム	—	本システムには不向き
	口コミ的情報提供	ウェブ上の日記から評判的情報の抽出	個人日記による名誉･信頼毀損問題	既存のシステムblogWatcher･問題研究済み
	評判情報の信頼性の問題	—	信頼性という概念の考察	考察検証済み

表 2.2: Penates評価-グループ１-

さらに，判断基準を考慮する上で必要とされる技術的対策の一つとして評判システムが挙っているが，これに関しても既存の研究を調査し，そこにおける問題を抽出することで，個人向けサービスにおける評判システムとしてどのようなシステムが必要

とされているかに関する考察を提供してあるので，研究・考察済みとした．

2.13.2 グループ２

次に，非技術的対策が必要とされているグループ２（表： 2.3）についてである．Penates をグローバルな取引がおこなわれる環境下で利用するとなると，プライバシという概念の共通理解が必要になる．個人情報を取り扱う上で，どのような情報の取り扱いに注意すべきか，という点において異なる理解をもっていると，それに対する対処法も異なってくるので共通理解が必要とされるということである．さらに，グローバルなガイドラインの必要性も取り上げ，現状のガイドラインについて十分な考察をおこなったので，この点に関しても検証済みとした．

Penates	問題提起	技術的対策	非技術的対策	完成度
グローバルな法的規制	文化の違い	—	プライバシという概念の共通理解の必要性	考察済み
	国境を越えた取引の規制	—	グローバルガイドライン	ガイドライン検証済み
セキュリティ	アクセス制御	統一した認証基盤	セキュリティ対策の脆弱性を指摘する技術の公表制限	システム未着手・制限は提案済み
	否認防止	デジタル認証・証明書	本人確認の必要性	共に研究済み
	安全性・機密性確保	暗号化技術	暗号文を平文に直す技術の公表制限	必要性実証済み

表 2.3: Penates 評価-グループ２-

セキュリティ対策に関しては，それぞれの必要な技術的対策に関しては，既存の研究状況を調査し，それに伴う問題として挙っている非技術的対策に関しては，どのような規制が必要とされるかということを提案した．

2.13.3 グループ３

グループ３（表： 2.4）においては，非技術的対策をバックアップするための概念を導きだすための論点なので，技術的対策は論じていない．この項目においては，ほぼ全ての論点において十分な考察が導きだされたと考える．著者としては，人間とサービスの関係という論点において，人がどのような関係性を築いていくのかという問題はまだまだ検討の余地が残されていると考えるので，研究中とした．

Penates	問題提起	非技術的対策	完成度
個人情報提供の判断基準	判断基準の不明瞭さ	心理学的判断基準	研究済み
人間とサービスの関係	どのように関係を築くか	生活をサポートするロボット的存在として	研究中
信頼性	信頼性という要素が技術の普及に関わる	提供される情報への信頼	研究済み
		セキュリティ対策に対する信頼	研究済み
		生活サポートシステムとしての信頼	研究済み

表 2.4: Penates 評価-グループ 3 -

2.13.4 グループ 4

最後のグループ 4（表： 2.5）は，今後新たな問題として考えられるであろう論点についてである．Penates をプライバシ保護を実現するシステムとして稼働させる時期が来る頃には，これら，個人情報を抽象化することや，自動で取得されてしまう情報に関しても注目が集まることになるだろうと考える．そこで，これらの問題も事前に検討しておく必要があると考えた．

Penates	問題提起	技術的対策	非技術的対策	完成度
個人情報の抽象化	個人向けサービスにおける情報の抽象化の可能性	匿名性を保った認証技術	抽象化の重要性	システム提案済み・概念研究済み
自動的に取得されてしまう情報	タグが情報を自動提供する	タグ機能の無効化技術	タグ利用の有効的な制限	共に研究中

表 2.5: Penates 評価-グループ 4 -

実際に，抽象化の問題としては，技術的対策として匿名性を保ったままの認証技術を提案し，その必要性を消費者に説くことを非技術的対策として挙げた．そして，自動的に取得されてしまう情報としては，自発的に情報を送信するタグを例にとって，それぞれの対策について研究中とした．

Penates においてこれらの要素がどうか関わってくるかというと，Penates は，情報の利用用途との比較を終えると，データベースから該当する情報を取り出すことになっているので，その段階で，情報管理をおこなっているデータベースが抽象段階を基に分けられている必要が出てくるのである．さらに，自動的に取得されてしまう情報に関しては，個人情報の自己管理をおこなう本システムを利用することが全くできなくなってしまうが，そのような状況かにユーザが存在していることは，検知できるはずなので，それを利用して，どのような情報が取得される可能性があるかをユーザに通知する役割をもったりすることが可能であると考える．

この結果を基に，将来課題を把握する．

第3章　九つの論点から導きだされたこと

本章では，第２章で論じた九つの論点から導きだせる，プライバシの保護が実現されるような環境を構築するために，２章で論じたような対策や概念とは別に，各個人が持つべき役割や，責任についての考察をおこなう．

前章では，それぞれの論点に関して考察を論じ，プライバシ保護を実現するためのシステムを構築する際，それぞれの論点に関し，どのような点に考慮すべきかを論じたので，本章では，その考察を検討する中で導きだされた，全体として誰が何をすべきかということに関して，消費者，企業，政府の三者それぞれの視点からまとめる．

3.1　消費者が考慮すべきこと

まずは，消費者が考慮すべきことを論じる．個人向けサービスをはじめとした新しい技術が普及することによって，誰もが生活の一部としてコンピュータを利用するような環境（以下，ユビキタスコンピューティング環境）におけて，消費者は，図 3.1 に表すようにさまざまな権利に守られていると同時に，他人の権利を簡単に侵害できてしまうという立場におかれている．

個人情報を取り扱うような環境において，消費者はまず第一に個人情報を自己管理するという権利を与えられているといわれている．しかし，実際には，自己管理をしなくてはならないという責任を負わされているのである．その上，言論の自由は自分の意見を公にしていい権利を提供しているが，誰もが保持しているプライバシ保護権は，自分がネット上に公表した情報によって意識しない中で侵害してしまう可能性があるという問題を持っている．実際に，プライバシ侵害や，信頼侵害等の問題は，侵害した人に侵害する意図を持っておこなったかどうかという点に重点が置かれるが，これはなかなか証明することが難しい．なぜなら，意思があるかないかは見た目で判断できるものでも，証明できるものでもないので，簡単に，悪意がないものとして許可してしまう前例を作ると，取り締まりができなくなってしまうからである．従って，インターネット上に何らかの情報を公表する際には，常に他人の権利を侵害する可能性があることをきちんと理解した上でおこなう必要があると考える．

消費者がすべきことの一番大きなところは，自分の行動に責任を持つという点である．インターネット上の書き込みに関しては，既に自分で責任を持つべきであるという話も出てきて入るものの，どこか他人事のように感じている人もいるのではないだろうか．

また，ユビキタスコンピューティング環境においては，自分で自分の個人情報提供に関して責任を持たなくてはならないので，自分がきちんと理解しない状態で個人情報を提供してしまった際に何らかの問題が発生しても，それは自分の責任であって，誰も責任を取ってくれないのである．企業側が消費者にきちんとした情報を明示的に提供できるよう努力する半面，消費者側も企業側が提示している利用用途等を十分に把握し，自分の判断で責任を持てる範囲内で個人情報の取り扱いをおこなうべきであ

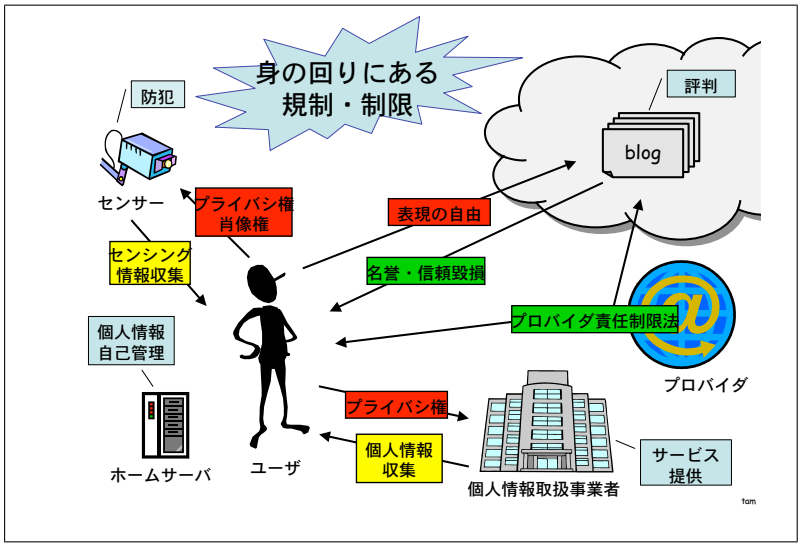

図 3.1: 消費者の立場

る．さらに，ネット利用に関して，自分がセキュリティ対策をしてないがために大勢の他人に多大なる迷惑をかける可能性があることも十分理解する必要がある．

本環境においては，如何にユーザに手間をかけさせないでユーザに適したサービスを提供するかというところが一つの大きな特徴となっているが，それは，一人一人がセキュリティ対策の重要さをきちんと理解した上で，十分な対策を講じているという前提の基に成立するものである．自分にとって悪いことが起こらなければ結果オーライという受け身な考え方ではなく，積極的に何かが起こったときのことを考えて十分な対策を講じているというプロセスを重要視して，万が一何かが起こってしまったときにはそのプロセスを重視してどうだったかという結果を導きだすような考え方に変えていく必要がある．これは，一人一人が考え方を改めないといけないので，現段階から自分が何をできるかということを考える必要がある．

3.2 企業が考慮すべきこと

ユビキタスコンピューティング環境構築において，一番重要な役割を果たすのが各企業である．技術の発展に伴ってさまざまな新しいサービスを提供し，それを浸透させていくためには十分な消費者の理解を得なくてはならず，企業・消費者・政府の三者が同様に協力しなくては成立しないとはいえ，その中でも企業の役割は中枢を担っていると考える．

では，実際に企業が果たすべき役割にはどのようなものがあるのかという点に関して論じる．役割の最大目的はユビキタスコンピューティング環境という新しい環境に対する消費者理解を得るためであるといえる．前節で，消費者の責任として，セキュリティ対策の重要性を理解したり，自らの行動に責任を持つべきであると論じたが，消費者がこのような責任を十分に認識するようにしむけるのは企業の役割である．では，その消費者理解を得るために企業がするべきこととは何か．大きく分けると，

1. 新しい形態のサービスに関する十分な知識を提供する

2. 安心して利用してもらえるような環境を提供する

の二点になるのではないかと考える．次にそれぞれに関しての詳細を論じる．

3.2.1 十分な知識の提供

まず始めに，一番重要なこととして，一般消費者に新サービスに関する正しい知識を十分に提供する必要があるということである．今後増えるであろう新サービスは，個人情報を要求し，その個人情報を利用することによって，よりユーザに適したサービスを提供できるようにするということで，個人情報の提供量とサービスのクオリティの間にトレードオフの関係が生まれることが予想される．これらのサービスは，一般消費者に利用してもらえなかったら何の役にも立たないので，どのような状況でどのようなトレードオフが生じて，個人情報を提供することで一般消費者にどのような利益があるのか，またどのような危険があるのかといったことをきちんと理解させる必要がある．

現状においても，個人情報を要求しているサービスは存在する．しかし，それらのサービスは，個人情報の利用用途を明確にしなければならないという法律に則って，消費者に分かる形で表示しているものの，実際にそれをきちんと読んで理解しているユーザはごくわずかであり，知らない間に利用されているというユーザが多くいる．また，余計なことを考えたくないから，自分に害のない範囲であれば勝手に利用してくれたほうがいいという考えのユーザさえも多く存在する．しかし，既存の一つ一つのサービスできちんとした理解を得られていない状況の中，ユビキタスコンピューティング環境の構築を進めるのは，極めて危険である．

今や，ほとんどの家庭でインターネット接続がされていると考えてよいだろう．企業はまず，インターネット契約をした時点で，消費者がネットワーク社会の一員になったのだということを認識させるべきである．そのためには，インターネット接続における契約時に，インターネットに関する知識のない消費者に対しては，インターネット接続における危険性についてや，セキュリティ対策の大切さ，どのようなセキュリティ対策があるか等と云ったことに関してレクチャすべきであると考える．これに関しては，それに関する情報を載せたハンドアウトを渡すのではなく，その場できちんと口頭で伝えたり，必ず読むように何らかの手段をとるべきである．細かい字で難しいことがたくさん書いてあるハンドアウトを渡されたところでそれをきちんと読む人はあまりいないと考えていい．従って，既存の方法のままでは現状のレベルを抜けられないので，一人一人がきちんと認識できるような環境を提供する必要がある．

インターネット接続に関して

インターネット接続に関する十分な知識というのは，ユビキタスコンピューティング環境に関する知識の取得のための第一歩であると考えられる．筆者が想定する環境において，全ての情報の取り扱いはインターネットを介しておこなわれる．従って，インターネットは現状における利用用途以上に，消費者の生活に密接に関係してくる．既にある技術を利用することから大きな抵抗を受けることはないと思われるが，現状の利用用途と同様に取り扱うとセキュリティの問題上，また個人情報を取り扱うという性質上，さまざまな問題点が浮かび上がってきてしまう．

サービスを提供したり，情報を提供したりする企業としては，コンテンツを提供するのみではなく，インターネット社会の一員としてすべきことを全てきちんと理解さ

せた上でサービスを受けられるようにするべきである．消費者がきちんと事情を理解した上で，そのサービスを利用するようにしむけるのは企業の役割である．

個人情報提供に関して

個人情報を提供することにより，自分に合ったサービスを受けられるようにするという環境下では，ユーザが自分の個人情報を自己管理するという点が重要であった．そのような環境下では，どのように自己管理をするかというところが問題であり，これは，企業が解決すべきポイントだと考える．

個人情報の自己管理のポイントは，個人が自分の個人情報がどのように取り扱われるかという情報を正確にきちんと把握するという点であった．このためには，個人情報が取り扱われる前に，その情報に関する利用用途等がユーザ側に通知されなければならない．しかし，偏在する全てのサービスからその都度いちいち直接ユーザに問い合わせが来るのでは，面倒であり，それでは自然にサービスを提供したいという当初の目的から外れてしまうため，できる限り自然にサービスが提供でき，且つユーザが個人情報を自己管理できるようにするため，Penates の実装をおこなった．本システム稼働時には，このシステムでサービスのポリシとの比較をおこなうことで，知らなくてすむ利用用途まで通知されるため，余計な警戒心を持たせることになるのではという懸念もあったが，そもそも知らなくてすむなら知らないままで済ませたいという考え方自体があってはならないものであるとの認識を持たせるように心がけたいところである．

3.2.2 環境の提供

次に，消費者が安心して個人情報の取り扱いをおこなえるような環境を提供するという点に関してである．自己管理がおこなわれるという前提において，問題となるのは，セキュリティ対策についてだと考えられる．実際に，自分の把握している範囲内でしか個人情報が利用されないということが保証されたとしても，悪意を持った第三者がデータベースに侵入したり，通信を妨害したりする可能性に関しても保証されない限り，消費者の信頼を得ることはできない．

実際には，暗号化や認証技術等によってセキュリティ対策は施されているものの，技術のみで完璧にセキュアな空間を保証することはほぼ不可能に近く，従って，穴がある箇所は法的に保証されるべきであると考える．法的な保証に関しては，政府がすべきことの節にて詳細を論じる．技術面では，論点２－２で論じた通り，機密性・完全性・可用性の三要素を基に，アクセス制御・否認防止・識別と認証が適切に実行されるよう試みるべきである．これらの基盤をきちんと整えてからサービス提供を検討すべきである．

現状において，個人情報取扱事業者[1]の不祥事が多く発表されている．これらは，今後増加するであろうコンテキストアウェアなアプリケーションの普及の障害となる．オンラインで提供したのではなく，オフラインで提供した情報でさえも，データベースで管理することによって，物理的に流出したり，ネット上で流出したりと云った問題が発生している．これは，オンラインで取り扱うようになったら指数関数的に危険が増加すると考えられ，人々のサービス利用意欲を消してしまう恐れがある．こういっ

[1]個人情報取扱事業者：一定期間の間続けて一定量の個人情報をビジネス目的で管理している企業・事業者等のこと

たことを防ぐためにも，前もってきちんとしたセキュリティ対策を講じ，消費者にその旨を理解してもらえるような環境を構築する必要がある．

最後に，個人情報を要求する際には，再度どの程度の抽象レベルまでが許容範囲かということを検証し，本当に必要な情報のみを要求するよう努めるべきである．抽象化レベルを明確にすること，匿名性を保ってもある程度のサービスが受けられるということ等を消費者に理解させることは，サービス利用意欲を増すことになる．また，きちんとした個人認証が必要な場合であっても，各サービス毎に認証システムを用意するか，どこか一カ所に認証の責任を持たせることで四方八方へ自分の個人情報を提供しなくてもいいようにするかと云ったことを早い段階で検証すべきである．

3.3 政府が考慮すべきこと

最後に，グローバルな視点での対策法を検討するには，一業界レベルではなく，国家レベルでの対策が必要とされる．個人情報を取り扱うようなサービスを広げていくにあたって，セキュリティ対策としてさまざまな技術が提案されているが，新しい技術が開発されるたびに，その技術を破る技術も考案されるため，全てを完全に技術で保護するというは不可能だと考えられる．従って，セキュリティ技術に対抗する技術を公表することを厳しく罰したり，セキュリティ技術を破って誤動作を引き起こした場合に罰したりする等，政府がそれなりの政策を打ち立てることが必要である．また，これらの政策を打ち立てる際には，国際的ガイドラインや他国の動向を把握した上で政策を検討することによって，後々変更しなければならないといったような自体を引き起こさないようにするべきである．

3.3.1 国内法制定

個人情報保護法に関しては，第一章で記述した通り，近年の技術の発展に伴って新たな法案が施行されている．しかし，現状のやり方だと，現状の法案で裁けない新しい問題が発生した後で，それに関する新しい法案を施行するという流れであり，法案は提案してから実際に施行されるまでに時間がかかるため，解決策は後手後手になり，問題は拡大してしまう．従って，政府当局には，問題が発生する前に，どんな問題が発生するかを考慮した上でそれに必要な法案が制定されるよう仕組みを変えることを期待する．

既存のさまざまな法案との折り合いをつけて，新たな技術によって起こる問題への対策法案を検証することは，非常に難しいことである．実際，言論の自由が制定された際，一人の表現・言論が簡単に世界中の人に配信されるという現状の状況は考慮されていなかった．従って，そういった新しい通信方法が主流になってきた今，既存の法案をそのまま押し通すことは難しくなってきているように思う．一度法律で認められた権利を覆すことは困難であるが，前提となる状況が変化した場合，既存の法案をそのまま押し進めるのは非常に危険であると言える．

以上のことを認識した上で，個人情報取り扱いに関する全ての国内法に関して再検討がおこなわれる必要があると提言する．

3.3.2 国際法の取り入れ

国際法の取り入れに関しては，OECD に加盟していることから，ガイドラインに沿った保護法を提案することができているが，自国が対策しているからそれでいいのではなく，まだ対策ができていない国に対してどのような処置をとるか，また，どのように対策を促すかということに関しても検討していただきたい．EU がきちんとした対策のない国相手にはデータ流通をおこなわないように定めているのがいい例で，そういった対策が我が国においても必要である．

インターネットの普及具合によって，国でのセキュリティ対策としての法制定の必要性が異なるのは否めない事実である．しかし，e-commerce はグローバルな視野を前提として進められていることから，グローバルなガイドラインを取り込むことの必要性は少しずつではあるが認知され始めている．また，国単位での政策は，法の施行に時間がかかったりさまざまな議論がされなくてはならなかったりすることから，GBDe のような，企業が中心となってグローバルなガイドラインを制定しようという動きがあることから，国としては，それらの団体を支援するような動きを起こしてくれることを期待する．

やはり，国交等の問題があったり法律といった国の政策で決定する問題があったりするため，各国のトップが集まって対策を立てることは必要だが，実際にグローバルにビジネスを展開している各企業のトップが集まって制定するガイドラインはよりリアルタイムなガイドラインになることは間違いない．なぜなら，彼らのほうが新技術や新サービスの問題に関してリアルタイムに対応できる立場にあるからである．

しかし，実際には，セキュリティ基盤を整えたり，認証基盤を整えるにはそれなりのコストがかかることから，一企業，一業界という単位では，必要な対策を講じることができないといった問題を抱えている．そこで，それらのコスト支援をおこなったり，一業界が基盤を整えようとしているときは，他業界もそれに続くように勧めたりと云ったようなことが政府・国の立場からおこなわれるよう提言する．

第4章　関連研究

4.1　TRUSTe

アメリカでは，TRUSTe と呼ばれるライセンシ制度があり，そのライセンスがサイトについていると，信憑性が高いと判断される．これは，２０００年３月に開かれた「政府による E コマースにおけるプライバシ問題会議」で全米弁護士協会に提出されたレポートであり，提示，選択，アクセス，セキュリティの四大基本要綱が定義されており，ここで定義された事項が忠実に守られたサイトがライセンシを取得できる．このライセンスを持つサイトは，個人情報の取り扱いに関して定義通りに取り扱いをおこなうことが保証されていることになる．

4.1.1　四大基本要綱

以下の四つの定義が TRUSTe のライセンシを取得したサイトが守らなけれならない事項である．

- 掲示
  どのような個人的情報が収集され，どのような人や集団に譲渡されているかを明らかにする旨を掲示する必要がある．また，この掲示は理解しやすく，クリック一つでホームページからアクセス可能でなければならない．
- 選択
  ネット利用者には，自分自身の個人情報をサイトが第三者に譲渡してよいかどうか選択する権利が与えられなければならない．
- アクセス
  ネット利用者が自分の個人情報を容易に訂正できるようにするため，一定のアクセスを許可しなければならない．
- セキュリティ
  一定の安全性を保証しなければならない．

4.1.2　TRUSTe-Watchdog

また，このライセンスは一度取得したら何をしてもいいと悪事を働かれることがないように細心の注意も払っている．例えば，あるライセンシが個人情報を乱用している，あるいは，表示しているプライバシ保護方針に沿った運営をしていないと消費者が感じた場合に苦情を提出することが非常に簡単になっているのである．これが Watchdog のシステムである．苦情がプライバシに関するものであり，問題のサイトがライセンシであれば誰でも利用可能であり，苦情が発生した場合，そのサイトには直ちに問題に対応する責任があり，TRUSTe は解決方法の調停に乗り出すこととなる．

このライセンスが民間に信頼を得ているのは実績はもちろん，この団体が非営利団体であることが上げられると考えられる．アメリカのインターネット利用者の中では最も信頼のおけるシールとして認識されている．

4.2 GBDe 提言書概要

インターネット技術の発展，コンピュータの小型化に伴い，ユビキタスコンピューティング環境の構築が進んできている．これに伴い，個人情報をネット上で取り扱う機会が増加したり，個人情報を必要とするようなサービスが増加してきた．

このような環境が構築されるに連れ，新しい問題点がいくつか浮上しており，これらを解決しないことには，ユビキタスコンピューティング環境の到来は考えられない．そこで，GBDe は以下のようにさまざまな視点から現状の問題点を抽出し，それらの対する解決策の提言をおこなっている．

なお，ここに記述されているものは，近年の提言書 [10] [11] [12] からの抜粋であり，本論文に関係していると筆者が判断した部分のみを抽出したものなので，詳細は提言書 [10] [11] [12] をご覧いただきたい．

4.2.1 個人情報保護

個人情報の保護については，サービス提供側が自己満足でプライバシポリシを公開するのではなく，消費者全体が意識するような環境を整える必要がある．一般的に，プライバシポリシが用意されていても，消費者はそんな免責条項の数々が細かい活字で書かれただけのもの等，うるさがるだけで読みはしない．

消費者の信頼を得るためには，これでは不十分であるということである．では，消費者の信頼を得るための個人情報の保護とはどのような点に重点を置いているのだろうか．ここではまず，２章に記した五原則や，提言の他に次のように定義されている．

個人データ

会社がオンラインで収集したデータで消費者を認識し得るもの，あるいは，他の入手可能なデータと容易に組み合わせることによって消費者を認識し得るものを云う．個人情報以外の情報として，どのようなブラウザを利用しているか，何回アクセスがあったか，発信源のウェブサイトのドメイン名は何か等といったような情報が収集されることがあるが，これらの情報が他の情報を組み合わさったとき，個人を特定できてしまうようなことがあれば，これらの情報も個人情報として取り扱わなければならない．

目的の明確化と公開性

OECD の定義とほぼ同様であるが，消費者への告知については，納得に値する告知をおこなうことと，消費者が自ら決定を下すのに足るに十分な情報を提供すること，消費者がそれを判断するのに必要な時間をきちんと設けること等が強く主張されている．

安全保障

会社はオンラインで収集した個人情報が，会社の内部の者によるか外部の者によるかを問わず紛失，不正操作，改ざん，不正利用や不正開示がされないように，納得のいく手段を講じなければならない．

4.2.2 裁判外紛争処理 (ADR)

国際的なインターネット取引に起因する紛争の裁判所への訴えは，適用すべき法律，及び，管轄権という難問によって複雑化される．また，コストもかかるので，実効的な救済が難しいと考えられる．

従って，司法に依らない魅力的な紛争解決手段を提供することで消費者信頼を得ることができるのではないかと云う考えのもと裁判外紛争処理が提案されている．この処理によって，政府行政機関や裁判所に訴えることによる遅延やコストを回避できるという利点がある．また，ADR の結果に不満がある場合には，法的な救済を求めるとの消費者の権利を保護する．

定義

物品の売り手またはサービスのプロバイダと最終消費者の間で (B2C)「電子的（主にインターネット）」におこなわれた契約に起因する義務に関係した紛争を解決する．解決方法には以下の三つがある．

- 仲裁
  当事者とは関係ない一人あるいは複数の仲裁者が，両当事者に事実及び彼らの論点を提出させ，最終的に公平性によるかまたは法律によるかして判断を下す
  - ほとんどの場合，当事者間の合意によって決定される
  - 最終決定である拘束力を持つ
  - 国境を越える B2C の，管轄権を超えた取引に簡単に適用されるのは困難
- 調停
  調停人が，両当事者が合意に達するまで，両者間で和解提案とその対抗提案のやり取りを単に相手方に伝えるという手続き
  - 調停人は交渉に干渉せず，最終合意を記録するだけ
  - 両者合意のもと成立した場合，その結果は法律上の契約であり，その効力の範囲内で執行可能
- 和解斡旋
  当事者とは関係のない和解斡旋人が公平な歩み寄りに向けて当事者を積極的に導く
  - 法的なものではない
  - 両当事者の法的権利及び義務についての理解は，勿論意味合いを持つが，それよりも，公平性が決定的要因となる

  - 両者合意のもとに成立した場合，契約として扱われ，その効力の範囲内で執行可能
  - 当事者が妥協点を見いだせない場合には，両者のいずれもが裁判所に持ち込むことは自由

この手法は，顧客満足システムとして考えられ，救済の段階の１ステップとなり得ると考えられる．また，ビジネス／消費者間での直接的な解決は，それが可能でさえあればB2C インターネット取引に関する顧客の苦情を解決する好ましい手段である．

インターネット上の業者への勧告

ADR は有効な解決策の一つではあるが，紛争の際の最初で且つ好ましい救済方法として，インターネット顧客にたいし，企業が運営する顧客満足システムへ申し入れる機会が提供されるべきである．しかし，十分な顧客満足が企業内のシステムによって保証されない場合には，紛争の解決を１つ以上の指定された ADR システムに提起する準備があることを通知すべきである．

また，注意すべき点としては以下のようなことが考えられる．

- ADR は紛争が生じた場合に顧客が自主的に取り得る一つの手段として提示されるべきであり，契約上の責務とされてはならない
- 業者は一般に，消費者をその結果に拘束する仲裁の利用を避けるべきである
  - 消費者の電子商取引に対する信頼を傷つける可能性があるから
- ADR 使用場合には，提起の条件，コスト，ADE の法的な性質，そしてその結果及びその他の審判所，特に法廷への関わり方に関して通知されるべき

ADR サービスプロバイダへの勧告

ADR サービスプロバイダサイドとしては，次のような点に注意すべきである．

- 公平性
  その決定が自主的におこなわれていることを認知されるためには，ADR 職員は公平でなくてはならず，これにより ADR を提供する組織の評価や信用を高めることになる
  - 適切に構成された関し組織の設置や，明確な基準に従った粉砕解決オフィサの任命等の適切な方法によって，公平性が保証されなければならない
  - 紛争解決職員は，紛争を解決する際に，業者及び消費者の圧力から絶縁されなければならない
- 迅速性
  いかなる場合にも，法廷よりも迅速に満足な結果を提供しなければ意味がない
- 消費者に取っての廉価性
  無償もしくは適度なコスト

- 透明性
  ADR プロバイダは，取り扱った総ての ADR ケース及びそこでおこなった判定の評価がおこなえるような年次報告を公表すべき
  - この際，特定の事件に関する情報及びデータの機密性を尊重すべき

政府への勧告

ADR のための法的な枠組みに関する研究により明らかになったことは，法的な枠組みは国際的な協定といくつかのレベル（連邦／州，地方／国など）での法律との間で分裂してしまっている，ということである．結果として，世界的な適用のために考えられた ADR システムは，多くの条件に配慮しなければならないのである．従って，GBDe は政府がこの勧告に沿った政策方針を採用することを期待する．

4.2.3 トラストマーク

GBDe では，消費者が信頼することのできる販売者を見極めることを補助するために，トラストマーク [6] 運動を支持する．また，消費者が異なった保護基準を提供するその他のトラストマークと混同することを避けるために，ガイドラインを制定した．

基本的に，トラストマークは，最低限の自主的なものであるべきと考えるが，以下の点については必須であると考える．

- 中小企業等にも手頃な費用で利用可能
- 明確な監視・報告システムを提供し，また強制に関わる判断の中立性を保証することにより，厳格に強制されること
- 容易なアクセス性
- 総ての利害関係者に意見を求める
- 悪用を防ぐための十分なセキュリティ
- ADR 提言に沿った消費者の救済メカニズムの提供

証明者に対するガイドライン

トラストマークを発行する側が考慮すべき点は以下の点である．

- アクセス可能性
  参加費用はトラストマークプログラムに参加することを妨げる価格であってはならないが，このことは付加価値サービスの提供についての設定を妨げるものではない
- 執行メカニズム
  証明者による無作為チェック，第三者による検証，販売者による定期報告を含むような，販売者の状況を監視するようなメカニズムを提供すべき

- 違反をおこなった場合の措置

  - トラストマークの剥奪
  - トラストマーク悪用についての公告
  - 政府当局への通報
  - トラストマークを掲げながらもプログラムの要件を破った販売者に対する訴訟等

- 視認性
  トラストマークは適切な場所に掲示されるべき

- セキュリティ
  証明者は消費者が本物のトラストマークと偽物を容易に識別できることを確保するため，明確で適切な措置を講じるべき

販売者に対するガイドライン

販売者側が考慮すべき点は以下の点である．

- 正確性と情報のアクセス可能性
  販売者が開示を要求される全ての情報は，明確，正確，且つ容易にオンラインアクセスできるようにする

  - 消費者にとって，誤解を与えたり，詐欺的または不公正になるような表示または隠蔽をし，或はそのような行動をおこなわない

- セキュリティ
  セキュリティに関する努力は最善の業界慣行に合致するものとし，収集され，保持され，第三者へ移転される情報の種別にふさわしいものであることとする

  特に以下を満たすべきである

  - 取り扱いに中止すべき，個人の財務情報や資料主審記録等の情報の授受については，最善の業界慣行を反映した暗号化措置を講じる
  - コンピュータに記録されているデータを保護するため，高レベルのセキュリティ措置をおこなう
  - 顧客との取引を満たすために使用する第三者に対しても，適切なレベルのセキュリティを保持することを求めるべく，合理的な措置を講じる
  - 消費者が取引を完了しない場合は，消費者の承認なしに消費者が特定できるような情報を保持しない

- プライバシ
  個人情報保護慣行に合致するプライバシポリシを公表し且つこれを守る

  - 告知／認識
  - 選択／同意
  - 正確性

  - 完全性／セキュリティ
  - 救済／内部ルール

- 依頼されていない E-Mail 発信
  消費者個人が opt-out できるようにする方針を守るべき

政府に対する提言

トラストマークプログラムは，消費者団体，主な会計関連団体，商工会議所等の業界団体及び企業による発展させてゆくものである．従って，政府干渉は時期尚早だと考えられる．

消費者信頼を高めるためには，まず民間ベースであるべきだと考える．また，政府の勧告や政府認定の強制によりトラストマークの調和を図る試みは，革新及び競争へのインセンティブを削ぎ，消費者信頼及び選択を損なう恐れがあると考えられる．

4.2.4 電子政府

民間企業の観点からみると，電子政府は，政府企業が有効性，スピード，品質共に優れた行政サービスを民間企業へ提供するのを可能にするものだと考えられる．電子政府とは，中央及び地方を含む行政，立法，司法の機関について，その内向，外向業務が IT 技術によりデジタル化，ネットワーク化に業務改革を含めて効率的に対応し，その質においても従来より望ましい水準にある状態という．

電子政府の実現は，企業の効率化，EC 環境利用を促し，EC 全体を発展させる．以下に，実際にどのような機能を持ち，どのような形態のものなのかについて記す．

モデル

インターネットを通じた政府と国民／政府と企業間の関係は，次のようなものであるべきだと考えられる．

- あらゆる個人情報の機密及びプライバシの保護に無条件に基づく
- 完全な安全性と信頼性の保証に基づく
- いつでもどこでも利用可能な完全に実行可能なオンラインサービスを提供
- 面倒な手続きを軽減し，国民がサービスを得るために訪問／相談する政府の省庁の数を最小限にする
- 異なる行政システム間の総合通信を容易にする
- 効果的且つ効率的，機動的且つ単純なものにする
- 多重チャネルを通じてあらゆる利用可能なサービスにアクセス
- 社会的に包括的
- 民主統治への国民の参加を拡大し，選挙手続きを改善

- 政府の構造を重視したものより，利用者を重視したものにシフト
- 政府が国民のニーズに応じたサービスを提供できるように独自化

起こりうる問題の可能性

現在の状況において，電子政府をたてるとなると，プライバシ，秘密性，セキュリティの欠如といったような問題が発生する．これは，法規制が，インターネットチャンネルの存在や，サービス提供のためのインターネットチャネルの独特な利用に即していないからである．

これらの問題を解決するために提供されるべき技術的ソリューションには次のようなものが考えられる．

- 公開鍵基盤，例えば，電子認証書
- 本人確認技術（バイオメトリクス，スマートカード等）等

提言

G2C：インターネットを通じて国民に提供されるサービスのプライバシ，秘密性，信頼性を保証する．また，国民が簡単にさまざまな情報にアクセス，提供及び交換できるように，電子政府システムは安全に保護されていなければならない．

国民のプライバシを保証し，国民に信頼を与えるために，政府がとっている安全対策をウェブサイト上で明示すること（これによって，e-service の総合的な促進にも役立つ）

グローバルな状況における電子政府

電子政府は最終的には世界中で同様に利用可能でなければ意味がない．そのために今の段階から検討すべき点は以下の通りである．

- できるだけ多くの言語に対応する
- 「技術標準」アクセス方法及びプロトコルについては，国際的に中立的水準の仕様や技術を採用
- 「管理規格」国際標準または世界標準規格を促進

4.2.5　インターネット決済

インターネットが形ある購入物の発注のみに利用されていたときには，支払いはその物品の配達時に伝統的手段を持って執りおこなうこともできたが，取り扱う物件がデジタル産品やサービスとなると，適切な支払い方法が必要となってくる．古典的な支払いシステムをオンライン環境に適用する上での問題点は，それらのシステムがインターネット上では提供されていないインフラストラクチャに頼っているということである．

現状

現在，ほとんどのインターネット決済システムは，クレジットカードまたは口座引き落としに基づいている．しかし，これらシステムはそれぞれ問題を抱えている．

- クレジットカード
  - 取引コストが高くなる
- 口座引き落とし
  - 国境を越えた取引には利用できない
- 共に
  - 暗証番号等の数字を入力した人物の特定はできない

現状のシステムでは，詐欺行為や信頼性における問題等，解決すべき数々の課題がある．しかし，実際には支払いシステムの市場は明らかに取り扱うビジネスの規模に支配されるので，どのような新しい支払いシステムもそれが既存のインフラを前提とするものでなければ出現が難しいという問題がある．

新しいシステム導入に対する問題としては以下のようなものが考えられる．

- 消費者による信頼感の欠如
- 消費者の習慣の変化の遅さ
- システムへの人々の関心を高めるのに必要な既存ユーザ数の不足
- 適切な基準の欠如
  - オープンでグローバルな標準の欠如
  - インターネット決済システムと従来システム間の相互運用性の欠如
  - 標準化された適切な消費者機器及び基盤の不足
- 国際貿易規則が調和してない
- 中央銀行システム間の相互運用の欠如

地域による特性

決算手段の選択は地域や商慣習によっても異なる．

- アジア・オセアニア
  - 日本では，B2C 決済においてクレジットカードに加えて現金引き渡しや銀行振込が一般的
  - 日本特有な現象としてコンビニを通してオンラインで注文し，支払いを受け渡しはコンビニでおこなう手法がある
- ヨーロッパ・アフリカ
  - フランス・イギリス

        * 小切手
    - ドイツ・スペイン
        * 電子送金，電子振替：取引コストが低減

- 南北アメリカ
    - 北米
        * クレジットカード，ElectronicBillPresentment and Payment
        * 顧客にとっての利点は請求書データと支払いを一括処理できる点

概観

新しいインターネット決済システムの構築を検討する際，一番始めに問題となる点は，十分なユーザ数の問題である．新しい決算システムに加入することは，販売事業者だけでなく顧客にも負担がかかる．十分な数のユーザを獲得できなければ，システムが如何に優れていても，加入のための費用が期待される収益を上回ることはない．従って，新しい技術は誕生しにくいのである．

そこで，従来のクレジットカード等が利用されるのだが，認証に問題があることから詐欺行為に直面することになる．これを解決するためには，共通の認証基盤を構築することが電子商取引の将来を左右する大きな課題となるのではないだろうか．PKIのように電子取引における認証を実現する基盤が存在していれば，その基盤の上にインターネット決済システムを構築できたと考えられるので，各決済サービスプロバイダが新しい認証基盤を独自に構築しなければならない状態にはならな以と考えられる．

また，ここでも同様に，グローバルな相互運用性を確保する上で欠かせない，国際貿易規則間の調整を図るよう強く勧告される．

さらに，固定インターネット決算とモバイル決算についても考慮すべき点が以くるかある．

- 固定インターネット決済の場合
    - ネットワークの接続状態等を考えて低コストでのインターネットアクセスが可能
    - 決算の際の認証に問題がある
- モバイル決算
    - モバイルネットワークサービスプロバイダと既に取引の関係があり，その関係をユーザの識別に利用可能

さらに，決算の問題を検討する上では公開鍵基盤および詐欺行為についての一般的見解を把握する必要がある．オフラインで利用されている決算システムをオンラインで使用することは，認証問題が解決されない限り不完全なままである．如何に挙げる項目は電子金融取引において不可欠な項目である．

- ユーザ認証
- データの完全性保時

- 支払い拒絶なきこと
- 取引データの機密性の確保

公開鍵基盤だけがこの問題を完全に解決できると考えられるで，今後はこの公開鍵基盤について重点的に検討すべきだと提言する．

現状では，単一のグローバル認証システムが確立される前に，最初の段階として国内の認証基盤が構築されようとしているが，このようなプロジェクトの推進者は，次の段階として国内基盤と云う「島」をつないでく可能性があることを意識すべきである．最終的には国境を越えての決算が実行可能となることが目標である．そのためには，各国は，法体系や決算方式に調和を持たせ，同時に中央銀行システム同士の相互運用性を確保すべきである．

インターネット決算に関する結論としては，安全性が保証され，かつ効果的な e/m 決算基盤は明らかな要件であるが，システムが十分な数の顧客や販売事業者によって利用されなければ，投資に対する見返りを得ることができないので，十分なユーザ数の問題が，インターネット決算システムの発展の最大の障害となっているということである．

以上を考慮して上での，GBDe の提言は以下の通りである．

- オープンな標準及び共通かつ相互運用可能な規格の策定を呼びかける
- PKI のような基盤の開発を政府が率先して支援するよう要請
  - もし政府が運営しない場合は，民間がインフラを構築するためにする努力が最小限で済むようにするため，法制度を改正すべき
  - 民間は，業界セクタを越えての推進団体を作り，基本概念の合意を目指すべき
- 初期手続きが簡単且つ効率的であること
  - しかし多少の手間は仕方なく，消費者も個人情報を保護するためにはたとえ手続きや操作に手間がかかっても必要なステップである点を認識すべき
  - 消費者団体もこのプロセスに加わり，消費者に対してこの信頼のためのインフラの利用を呼びかける
- 各国政府が決算形式の調和を図り，中央銀行システム同士の相互運用性を保証するよう要請

4.2.6 知的財産権

ブロードバンド時代の開始によって，以前は不可能であった方法による知的財産権へのユビキタスなアクセスが可能になった．しかし，知的財産の侵害問題は，世界的なオンライン上でのコンテンツ配信の持続的な発展を危うくするものである．

直接的な侵害者の責任

まず始めに，権利者が，権利行使するために必要な手段をとるためには，侵害者とされるものを特定することが必要である．では，実際にどのように侵害者を特定する

かという点においてだが，IP アドレスやドメインネームのような技術データは，知的財産権侵害の操作において重要視されるが，通常これらのデータはオンラインサービスプロバイダのような第三者によって管理されている．そこで，これらはサービスプロバイダにとって負担にならない程度に法執行機関に利用可能でなければならないことになる．

しかし国際的に考えると，これは，各国のデータ保護法によって一定の制約を受けることになる．我が国においては，この件に関しては付録 D に記載してあるプロバイダ責任制限法において定義してある．また，この制限法に従うためのガイドラインとして，プライバイダ規制ガイドラインが存在するので，それに関しては付録 F に記載した．

実際に，データ保護のルールは，データの保存や保全等の知的財産権のエンフォースメントにおける必要性も加味して解釈されるべきものだと考えられる．

刑事法におけるオンライン侵害の定義

コンテンツ流通の形態の変化に伴い，どのような行為が刑事罰の対象となる侵害に当たるかを明確化する必要が生じる．刑事法上の侵害については，知的財産権の故意の侵害行為が定義の出発点にあるべきだと考えられる．また，侵害者の主観的な動機は，商業的利益が直接的か間接的か，また単なるいたずら目的かを問わないこととする．

知的財産権を保護する技術的手段の回避の禁止

デジタル環境において知的財産権を効果的に保護し，秩序ある合法的な電子市場の発展を可能にするために，広く認められるような業界主導型の標準的な技術的手段，及び 1996 年の WIPO 著作権条約及び WIPO 実演・レコード条約の完全履行を達成する法的な枠組みが重要な要素である．

問題は，技術は，それが十分に確固とした信頼に足るものでなければ，ハッカーや海賊の攻撃に対して脆弱という点であり，このため，技術だけでは，著作物を非合法的な複製や領布から守ることはできないのである．そこで，米国は，DMCA[15] によって WIPO 条約を導入し，日本は，1999 年の日本著作権法 (JCL) によって WIPO 条約を導入した．f

DMCA，JCL，EUCD(EU 著作権指令) においては，迂回行為，及び迂回機器の製造，輸入，提供，公衆への領布を禁ずる制度を採用している．そのような機器と部品は，技術的保護手段の迂回を可能にするという目的で設計，製造，販売，領布する範囲に限って禁止され，また，迂回行為以外に限られた商業的な目的あるいは用途しかないのである．

一般原則は次の通りである．

- 適用範囲
  あらゆる形態のコンテンツを特定，保護，管理するために用いられる標準的な技術手段の策定を促進

- 自主規制と標準化
  オープンでグローバルに調和した技術的コンテンツ保護標準の制定に対して適切で迅速な方法で，政府が助成することを支持

- 特定の例外
  迂回行為禁止義務の例外や制限は綿密に検討し，迂回行為禁止の妥当性と有効性を維持しなければならない
  - 迂回行為禁止義務の例外は，基本的な禁止事項に影響を与えるほど，また迂回機器の公衆への販売や領布を許可するほど広範に渡ってはならない
- 著作権補償金
  技術的保護手段を効果的に講ずることによって得る明確なメリットの一つとして，著作権補償金の課せられる国で著作権補償金に対する必要性と法的制度がなくなることであると考える
- 容認及び不干渉
  そのような枠組みの場合でも，インターネットサービスプロバイダに自分たちが送信または保存する情報をモニタする義務を課してはならず，各種の関係者に不当な負担を課してもならない
- 著作権管理技術
  ウォータマークを初めとするコピー制御技術では，コピー制御・コンテンツ管理情報をコンテンツそのものに埋め込むことができる
  - エンドユーザにコンテンツが届くまで領布網のあらゆるポイントで，コンテンツを確実に保護する助けとなるよう設計されている
  - 再生装置と記録装置が適切に対応し，且つこれらの技術の保全性が守られ，エンドユーザにコンテンツが届くまでに効力が失われない限り，こうした技術によって不法なアクセスやコピーが効果的に防止される
- インタオペラビリティ
  コンテンツとともに移動するコピー防止と管理に関する情報の完全性，及びネットワーク運営の完全性と効率を維持するような方法で，さまざまな技術の間で相互に連携動作が可能とならなければならない

結論としては，知的財産権を保護し，インターネットやその他の世界的な領布システムにおける著作物の領布を管理する能力を高めることにより，著作権者は，デジタル環境においてより多くの質の高い著作物を提供するのを促進するであろうということである．またその結果，消費者はより多様で広い選択をすることが可能となり，合法的に質の高い作品にアクセスしやすくなる．

4.2.7 インターネットの未来

インターネット利用が進化するに従い，重要な新しい課題が登場することがますます常態となりつつある．そこで，GBDe は，ブロードバンドとサイバーセキュリティに関するこれまでの提言を，国際環境の変化を考慮して更新した．加えて，RFID を政策立案者と実業界がともに注意深く考慮しなければならない可能性を持った課題として取り上げた．

インターネットが持つ経済的なポテンシャルを十分に実現させるためには，プロードバンドネットワークが広く利用可能であり，その利用が広がることが極めて重要な

要因となってくる．利用者にさまざまな革新的なサービスやコンテンツを，競合するが相互接続性のある複数のオープンなプラットフォーム上で提供することが望まれる．

4.2.8　サイバー倫理

インターネットは，既存の国境，管轄及び適用法を越えて広がるため，伝統的な法律や規則の中では，これらの問題に効果的な解決手段を見いだすことは極めて困難である．言論と表現の自由，並びに芸術や報道の自由を十分に保護しながら，国境を越えた産業界の自主規制を通じてインターネット上の非倫理的なコンテンツの流通を積極的に防止し，利用者のためにフィルタリングやラベリング・ツールを提供し，政府当局や他の資格ある組織と協力して本問題を周知させることが重要である．

利用者に関する原則

現在の利用者や将来のサイバー市民にメディアの能力とサイバー倫理を広く伝えるためのプログラム作りを支援すべき

政府当局に関する原則

言論と表現の自由を国際レベルで保護する一方，倫理に反したコンテンツがインターネット上を流通することを防止する公的機関と民間による活動を調整するために，産業界は国際的または地域的な組織との建設的な対話に参加しなければならない．また，各国の国内法及び慣行に従い，かつ，基本的権利，特に言論の自由を尊重し，産業界は，インターネット上の犯罪または違法なコンテンツの調査において，引き続き法執行当局に迅速に協力すべきである．

4.2.9　サイバーセキュリティ

サイバーセキュリティは思想及び理念を交換する自由，情報の自由な流通，情報及び通信の秘密，個人情報の適切な保護，公開性並びに透明性を含む，民主主義によって認識される価値と合致する方法で実施されるべきである．また，これを実現するために，インターネット参加者の全ては，情報セキュリティの必要性を認識し，セキュリティを高めるために自分達に何ができるかを知らなければならない．

サイバーセキュリティの重要な課題の一つは，サイバースペースにおけるあらゆる脅威と戦い，電子商取引における利用者の信頼を保護することである．

セキュリティ文化

B2C 電子商取引が発展するに連れて，市場は重要インフラとして機能を持つようになり，セキュリティ障害は大きな打撃になる可能性も出てくるので,「企業のセキュリティ」の範囲は企業内だけではなく消費者や取引の関係者にまで及ぶ　また，企業自らの責任を認識し，役割を果たすだけでなく，個人ユーザレベルでのセキュリティの実践についても，企業が果たすべき役割は非常に大きいと考えられる

- 企業のセキュリティ
  企業としては，情報システムやネットワークに関する脅威や脆弱性に適切に対応することによって自らの資産を守ると同時に，自ら設備を安全に保つことによって社会全体のサイバーセキュリティを確保すべき

  - 企業内のセキュリティを十分なものとするための四つのレベル

    * エグゼクティブ
      CEO 等によるセキュリティポリシを制定し有効に運用することによる首尾一貫した対応
    * ネットワーク管理者
      エグゼクティブの正当な指揮の下 OECD ガイドラインの「セキュリティの設計・実装」の原則を重視し，実施する
    * 社内ユーザ
      社内ネットワーク利用においては，ガイドラインに従い，不正利用をしてはならない
    * 社外ユーザ
      企業は，電子商取引のセキュリティを確保するためには，顧客だけではなくインターネットサーフィンをしているユーザも企業のセキュリティの範囲として考慮する必要があるが，その際注意すべきは以下のポイントである
      1. 企業に近いユーザと一時的なユーザを区別することによる，個人ユーザとの関係を再検討
      2. サイバーセキュリティに関する企業とユーザの関係の定義，公表された契約事項による相互責任の提示
      3. サイバー攻撃に対する定期的な状況報告と情報更新
      4. 個人ユーザに関わるセキュリティ脅威への対策
      5. 企業のヘルプラインやコールセンタにおけるセキュリティの認識
      6. セキュリティ対策の広い周知

- 社会全体でのセキュリティ
  サイバーセキュリティは，IT の世界だけでなく，経済社会システム全体の中で考慮されるべき

  - 社会全体として適切なレベルのセキュリティが必要

    * 電子商取引や電子政府のメリットを安全に享受できるような適切なレベルでのサイバーセキュリティが世界的に確保されていることが必要
    * セキュリティの必要性をネットワーク社会の市民・企業・政府が等しく認識し，そのために必要な対価をそれぞれで分担すべき（それぞれがそれぞれの立場しか考えなかったら全体的に低下する）

  - 投資に見合ったセキュリティ
    ユーザは相当するコストを支払うことによって自分の求めるセキュリティレベルのサービスや機器の提供を受けることができる一方，サービス提供者はクライアントの求めるセキュリティレベルに応じて，幅広くセキュリティ関連機器，ソフトウェア，アクセス等のサービスを提供するべき

- 個人ユーザの役割と企業
  電子商取引の市場で個人ユーザは顧客あるいは加入者として企業のセキュリティにも密接な関連があるので，個人ユーザにもサイバーセキュリティに果たす役割はある
- セキュリティの標準化
  いかなる特定の管理・認証の方法を推薦・支持することはなく，管理・認証に関するセキュリティ標準がグローバルなベースで政府，民間の活動によって採用され，運用されることを提言し，また，秘密情報の保護，ネットワーク・セキュリティ，取引の安全性について，最低限の基準の保証に向けた法的条件の整備は新興国・地域がおこなうことを推奨する

課題

サイバースペースにおけるあらゆる脅威と戦い，電子商取引における利用者の信頼を保護することが重要な課題の一つである．電子商取引のセキュリティが世界的に確保されるためには，認証基盤の確立が重要であり，これが全ての国の人々に提供されるべきであると考えている．また，認証基盤を通して実現される，ネットワークと情報システムのセキュリティに関する属性は，以下の通りである．

- 認証
- 非否認性
- 完全性
- 秘匿性

情報技術の進歩に伴い，認証サービスが多くの利用者に提供され，ディジタル署名を法的に認める枠組みを制定するため，各国政府はディジタル署名・ディジタル認証に関する法律を制定し，執行してきた．多くの場合，公開鍵基盤 (PKI) によって提供される認証サービスは以下の２通りの形で提供される．

- 政府による提供
  電子政府の重要な構成要素
- 民間事業者による提供
  民間事業者が用途別の証明書ポリシに従って認証サービスを提供

もし企業や消費者が非常に多くの証明書を使うことになった場合，電子商取引を妨げる脅威が潜在的にあると考えるので，不便性を解消するため，認証サービス事業者は，相互認証協定を通じて他の認証局を認証することができる．

- 実際に証明書を発行しないでも，他のメインのルート認証局を「信頼できる」と宣言することによって相互承認できる

提言

認証サービス事業者が相互認証協定 (MRA) を通じて認証局を相互に認証すべきである

- 相互認証のモデル相互認証とは,「二つの認証局が相互に相手を認証するプロセス」
  - お互いのセキュリティポリシが同等のセキュリティレベルにあることを確認
  - 認証サービス事業者が，ルート認証局として信頼する第三者に従い，この第三者を通じてお互いを認証する
- 認証局の責任（法的問題）エンドユーザは証明書の不正使用や，不正アクセス，暗号解読による個人譲歩の漏えいによって被害を受けることがありうるので，相互認証による責任問題を明確にすることが提言される
  - 国際的に議論される場合，認証局の免許制度，ディジタル署名法，暗号規制などの各地域の法的システムや，商取引勧告が考慮されるべき

4.2.10 RFID

RFID 技術は情報化社会に重要な意味合いを持つ．この技術は，効率を高め，在庫管理を革新し，製品デザインとマーケティングを改善するポテンシャルを持っているが，この技術がデータの収集，モニタリング，と保存に関してプライバシ問題を起こしうつことも念頭に入れるべきである．

- 物理的な世界とヴァーチャルな世界を結びつける

将来性

既に，個人情報保護，相互運用可能性の確保，標準化等の課題が重要であると認識されている．

- 個人情報保護
  RFID を用いた故人を追跡したり，個人の購買パターンに関する情報を収集したり，個人の安全が脅かされる危険性を懸念する声がある
  - 消費者の側に情報のコントロールをもっと与えることと規制によるコントロールのバランスによって解消可能かも
- システムの信頼性
  RFID タグからのデータが盗聴されることや，不正な改ざんを被る危険性
- 消費者への教育
  RFID 利用がもたらす便益を理解できるように，正確な情報が提供されるべき
- 標準化
  製品識別，タグとのデータ通信，製品とそのステイタスを記述するための諸標準の調整と採用が必須
  - 標準化なしでは，RFID タグのコストが幅広い利用の妨げとなる

4.3 アメリカにおける人々のインターネットに対する信頼に関するアンケート

人のインターネットに対する信頼感について論じた際に，参考にした資料の詳細において，自分の研究を考察する上で重要視した項目についてまとめる．

このアンケートでは，今やアメリカにおける大半の人がインターネット利用者であることを背景とし，始めたばかりの人から，インターネット利用に慣れ親しんでありベテランと呼ばれるような人まで幅広く対象をもってアンケートを実施した．これにより，ユーザが何を求めているのか，ネットをどの程度信頼しているのかということに関する考察を導いている．

4.3.1 Matter of Trust: What Users Want From Web Sites

ユーザがサイトに求めること

- ナビゲーションがわかり易い
- 欲しい情報が見つけ易い
- サイト上の情報に信憑性が高い
- サイト上の情報がタイムリーに更新されている

サイトに求めることでパーセンテージが低かった項目

- オーナーが明確であること
- サイトを金銭的にサポートしている組織，企業に付いて
- 第三者からの評価・評判

e-commerce なウェブサイトに求めること

- 取引をおこなう上でかかるすべての費用（搬送料や，取引コストを含む）
- 提供した個人情報を如何に利用するかに関する詳細な情報
- 自分が購入した品に関する情報：いつ手元に届くか，自分の予約情報等
- 予約解除や，返品に関するポリシ
- 何らかの問題が発生した際に，直接尋ねていけるような連絡先に関する情報
- プライバシポリシ

ユーザが知りたいこと

- 誰がサイトを運営しているのか
- 運営者にどのようにコンタクトをとれるのか

- サイトのプライバシポリシ
- 間違いに対してどのように対処するのか
  - 過ちに関しては，過去にどのような問題があり，それをどのように対処したかという情報を載せたページが欲しい

問題だと考えられること

- サーチエンジンの結果が必ずしも中立性を保った上での結果ではないという事実をユーザがわかっていない
- プライバシポリシ情報を要求する割には，その情報がどこに掲載されているか探そうとしていない
  - 実際には，ネット上の”About Us”で公表しているが，それを知っていても読んでいるという人は少ない
- 第三者が信頼性を保証するシールシステムがオンライン上で未だ十分に浸透していない

ベテランと初心者

サイトにアクセスするために，要求される個人情報に関して，大半のユーザが抵抗はないという結果をだしている．また，ネットアクセスの際には，cookies が稼働するが，それに関する知識をユーザがどの程度持ち合わせているかという点に関しては，オンラインの経験値とそれに関する知識の間には強い関係が認められる．同時に，ネットにおける信頼という点でもネット経験が大きく影響してくることがわかった．

男性と女性

インターネットに対する信頼感，危機感の持ち方，対処に関する考え方等は，男女の間でも違いが出ていることがわかった．このアンケートによれば，男性のほうがセキュリティに関して関心を持ち，一定の対策を施しており，さらに，十分な知識を持った上で e-commerce を利用している．

しかし，この差は，ネットを家とオフィスの両方で利用する人と，家でしか利用しない人の間に生まれる差でもあることから必ずしも男女の間で生まれる差ではないのではと考えられる．

信頼感に対する考え方の違い

実際にクレジットカード等を利用して，インターネット上で決算をおこなっているユーザとそうでないユーザとの間には，ネットに対する信頼感に違いが生じている．実際に利用をした上で，また，仕組みを理解した上でネットに関して心配や疑いを持っている人と，そうでない状況で，ただ心配や疑いを持っている人との間には，同じように懸念を持っていたとしても，種類が異なるということが読み取れる．

クレジット等の利用に関しても，インターネット経験が長ければ長いほど，教養が高ければ高いほど利用しているという傾向にある．ある程度の仕組みを理解した者が，その上で，自分の利益と危険を把握した上でシステムを利用していることが多いと考えられる．

これに関する詳細は A Matter of Trust: What Users Want From Web Sites [25] を参照頂きたい．

4.3.2 Trust and privacy online: Why Americans want to rewrite the rules

アンケートから導きだされたデータ

- ２４%のユーザが自分の個人情報を提供する代わりに虚偽の情報を提供している
- ２６%のユーザが自分に覚えのない相手から来たメールに関して返信している
- ９%のユーザがメール利用の際に暗号技術を利用している
- ２５%のユーザがコンピュータがウィルスに感染した経験がある
- ４６%のベテランユーザがクレジットカード利用に関して心配を持っている
- ７０%の新米ユーザがクレジットカード利用に関して心配を持っている　等

結果導きだされたこと

- アメリカ人は，自分のプライバシが保証されることを望んでいる
  - 個人情報を提供する際には，”opt-in”方式で尋ねられたい
  - 自分がいつどこでと云った情報を制御できるのであれば情報を共有することも苦ではない
  - 消費者教育が，ユーザの疑心を拭うための要素である
- プライバシ保護のためのゲリラ方式
  - 虚偽の情報を提供する
  - インターネットという世界が，”public”と”private”をきちんと分けて理解することを望む
- 罰について
  - 個人情報が違法な使い方をされた場合は，罰を与えるのが当然であるという意見が多数
    - 刑務所に入れる
    - 逮捕させる
    - 違法利用した旨を公表する　等
  - ソフトの違法コピーは”海賊版”と呼ばれ違法扱いされるのに，個人情報の違法コピーや利用は ”共有 ”と呼ばれるのはおかしい

- 恐怖と信頼
  - クレジットカード利用の際に起こる心配は，オンラインでもオフラインでも変わらない
  - メールが関係のない第三者に改ざんされたり，読まれたりするのではないかという心配
  - ウィルスや未承諾メールに関する心配
  - きちんとシステムを理解した上での有効利用
    * オンラインカレンダーやアドレスブックの利用
    * TRUSTe マークによってプライバシ保護が保証されているサイトがより頻繁に利用される
- プライバシに対する懸念はなぜネットのポテンシャルを制限するのか
  - ネット利用の経験が長いほど，ネットセキュリティに対して信頼を持てている

  従って，懸念を持つことによって，知識を得ることになれば，必ずしもポテンシャルを制限するとは限らない.

さらに詳細を知りたい場合は，Trust and privacy online: Why Americans want to rewrite the rules [26] を参照していただきたい.

第5章　将来課題

5.1　Penates 将来課題

将来課題としては，第２章最後でまとめた Penates の評価の際に，まだ完全に終わりきれていなかった部分に関しての研究を進めることである．

- 判断基準を提供するシステム
  まず，評判システムの口コミ的情報を提供するシステムである．このシステムは，既存のシステムとして blogWatcher というインターネット上の全ての日記サイトをクローリングして，その内容を解析することにより，何らかのテーマに関する評判情報があったらそれを提供するというものである．しかし，言語解析の問題のみならず，評判情報として提供するだけの情報量が必ずしも確保しきれているわけではないという問題や，個人の日記内容が他人に与える影響がより大きくなることから，自分で提供する情報に関する責任が重くなるといった問題が発生している．将来課題としては，この問題への解決策を検討すると同時に，ユーザが最も強く求める評判情報とはどのような種類のものか，また，どのように情報を収集することが最適であるのかといった問題も検討すべきである．

- グローバル基盤
  グローバルな取引がより繁栄してくることは、もはや疑いようのない事実になりつつあるので，これを考慮した上で，グローバルな法的規制に関してどのように取り組んでいくか，再度検討が必要であると考える．背景や文化の違いは，前に説明したように概念の把握さえも異なるものとしてしまうのである．

- セキュリティ
  セキュリティの問題は，今まさにさまざまな技術的解決策が検討されている所なので，現状としては，論点２－２で論じたように，脆弱性に対する対応策を十分に検討した上で，匿名性を利用した認証システムの導入を考えることで，できる限り完璧な環境に整える必要がある．

- 人とサービスの関係性
  ２章のグループ３において，信頼性という要素や個人情報提供の判断基準という要素は十分に考察したが，人とサービスの関係についての研究は，生活をサポートしてくれるロボットのようなアプリケーションの登場を検討している研究者にとって，非常に重要な要素となってくるのである．従って，この分野に関する研究は将来課題としてさらに追求されることが必要であると考える．

- 新技術への対応
  新しい問題点として，個人情報の抽象化の問題と，タグのように自動的に情報が送信されてしまうような場合の問題についていくつか提案したが，これらの

問題は日本国内において，まだそれほど大きな問題になっていないがために取り上げられていないだけで，少しずつ話題を呼ぶようにはなってきているので，大きな問題となって取り上げられる前に十分な対策が施される必要がある．

5.2 フレームワーク将来課題

最後に，九つの論点について考察をまとめる過程において，消費者・企業・政府の三者が，プライバシが保護されるような環境を構築する上で，どのような役割を持ってどのような責任を持っているのかということが導きだされたことから，将来課題として，その役割・責任をはたすために，どのような対策を講じることができるか，ということも把握する必要があると考える．そこで，これらの要素を本研究で提供したフレームワークに組み込むことで，さらに詳細なフレームワークの提供ができるようになることを望む．

第6章　結論

インターネットの普及や，デバイスの小型化等，さまざまな新技術の誕生や発展に伴い，技術者はさまざまな新しいサービスを一般消費者に提供することができるようになってきた．固定電話から携帯電話への移行等，新しい技術の発展は我々の生活をその都度変化させてきた．近年では，インターネットの普及に伴いさらに我々の生活がサポートされるようになってきた．これらの技術がさらに進化し，更なる新しい技術が組み合わされることで，我々の生活がさまざまな場面でコンピュータによってサポートされるユビキタスコンピューティング環境が構築されつつある．

しかし，ユビキタスコンピューティング環境の実現が，今までと異なる点は，新しいサービスを利用するために，利用者の個人情報が必要とされるという点である．今までの発達は，常に我々の生活に役立つサポートを一方的に提供してくれていたが，今回は，我々が自分の情報を提供することによって，その個人に合ったサービスが受けられるという個人向けサービスが登場したのである．従って，新しい技術の利用方法を習得するだけで，そのサービスの恩恵を受けられていたが，今後のサービスは自ら自分の個人情報を提供しなくては恩恵は受けられない．また，その性質上，個人情報の取り扱いがインターネット上でおこなわれることになるので，個人情報の漏えい等さまざまな問題が発生する恐れがある．

そこで，このような環境下で，個人のプライバシを保護するためのシステムを構築するためには，どのような点を考慮しなければならないのかを認識するため，個人情報を取り扱う上で重要な九つの論点を挙げ，これら一つ一つに対して考察を導くことで，プライバシ保護を実現するためのシステムを評価するためのフレームワークを提供した．

さらに，実際にプライバシを保護するためのシステムの一部として実装した Penates をプライバシ保護システムとして完成させるために必要な要件を上記フレームワークを利用して評価した．これをおこなう上で，このようなシステムの構築を検討する際には，技術的視野からのみならず，法の改正や，社会学等非技術的視野からも問題を検討することが必要であるということがわかった．

加えて，これら九つの論点から導きだされたいくつかの対策案は，開発者側が検証すべき問題だが，研究者が対応すべき要件以外にも，一般消費者が対応すべきことや政府が対応すべきことが導きだされた．消費者は，自分達の個人情報を自己管理することの重要性を十分に理解し，それに伴うセキュリティ対策をおこなうべきである．また，サービスを提供する企業のみならず，一企業，一業界という枠を超えて，社会全体でセキュリティ対策の重要さを認識し，一般消費者にそれに必要な知識を提供できるような環境を整えなければならない．最後に，社会全体で対策を施すことができるように国が政策を立て，企業の対策をバックアップする体制を整えつつ，一国という枠にとらわれずにグローバルな視点で政策を施すことが必要であると考えられる．

謝辞

約三年半に渡り，自分が興味を持った分野の研究を思うままに進めていく機会を与えてくださり，幅の広い知識を得るために，国際学会に参加する機会を与えてくださった早稲田大学理工学部中島達夫教授に深く感謝いたします．

また，所属グループが異なるにも関わらず，研究の方向性や発表構成など，自分が悩んでいる際に，時間を問わず一緒に考え，アドバイスを与えてくださった早稲田大学理工学部石川広男助手に感謝いたします．

更に，昼夜を問わず，共に悩み，励ましあい，笑いあった，同輩の安達・生形・小林・鈴木・中村・松浦・山邉氏にこの場を借りて御礼申し上げます．長い間，大変お世話になりました．

そして，修論の言葉遣いのチェックや，内容の矛盾，図の表現の仕方など，修士論文を書き上げるにあたる全ての工程において，いろいろとご指導くださった中島研究室の皆様に，厚く御礼申し上げます．

最後に，六年間大学に通わせくださり，常に温かい目で見守っていてくれた家族に深く感謝いたします．

付 録A　ポリシ・マッチングシステム

論点１－１で紹介した，各個人が自分の個人情報を自己管理するためにシステムであるポリシ・マッチングシステムについての詳細を以下に示す.

A.1　ポリシファイル

ポリシファイルは，サービス提供側が，ユーザに合ったサービスを提供するために，どのような個人情報を必要とするかについて記述したファイルである．サービスには，いくつかの段階があり，より多くの個人情報を提供することによって，よりクオリティの高いサービスを提供することが可能となる．しかし，ユーザに取っては要求されている個人情報の種類によっては，高いクオリティのサービスを望まず，最低限のサービスのみを希望する場合もあるので，どの個人情報をどのような利用目的で，誰がどの位の期間必要とするかということを詳細に定義したファイルが必要となる．従って，それらが詳細に定義されたファイルがポリシファイルという事になる．

一つの個人情報を複数の利用目的で利用したいと考える場合もあるが，その場合は，各利用目的毎別々に定義することが必要とされる．また，情報利用者については，基本的に要求される個人情報は，サービスを提供するために必要とされるのだが，場合によっては，マーケティングなどのために個人情報を利用したいと考える場合もあり，その場合は収集した個人情報を第三者に提供してそれによってマーケティングをおこなうということも考えられる．このような場合には，付録 A で詳細を記載したように，個人情報保護法によって，個人情報を第三者に提供するためには，その旨を事前に所有者に確認をとる必要があるので，ポリシファイルによって適切に定義しておく必要がある．

以下はポリシファイルの一例である．属性の description にどんな個人情報がどのような目的で利用されるかを定義しておくことによってユーザに情報を与える時に，渡しやすいようにしてある．ここでは，ユーザのロケーションがこのサービスの当初目的達成のために必要とされ，ここで収集されたロケーション情報は情報収集当事者によって，半永久的に保持されることが定義されている．

```
<STATEMENT description="Service collects
user's location for marketing">
  <PURPOSE><current></current></PURPOSE>
  <RECIPIENT><ours></ours></RECIPIENT>
  <RETENTION><infinit></infinit></RETENTION>
  <DATA ref="#user.location"></DATA>
</STATEMENT>
```

A.2 プリファレンスファイル

プリファレンスファイルは，ユーザ側が用意すべきファイルである．このファイルには，ユーザが自分の個人情報を提供する条件として，どのような利用目的なら許可するか，また，どのような場合は提供を拒否するかについて記述してある．この定義ファイルによって，すべての個人情報が三つのカテゴリに分けられることになっている．その三つとは，許可，拒否，通知の三つである．許可のカテゴリに定義された個人情報は自動でサービス側に提供することが許可されているもので，拒否は同様に提供が拒否されているもの，通知はその時々によってユーザがに直接選択を任せるように，要求されたことを通知するようにということで定義されているものである．

現在，買い物の際に必要とされるカスタマサービスのためのカードなど，すべての店ごとに毎回消費者はほぼ同様の項目についての記述を要求される．しかし，実際には同じ内容のことを聞かれているわけで，人によっては，そこに記述する内容は店によらず一定だと考えられる．そこで，事前にこのような場合は，どの程度の情報を提供することを許可するかについて記述しておくことで，毎回自分が記述しなければならないといった手間を省くことができると考えられる．

例えば，カスタマカードを作るだけの目的のためなら，住所氏名年齢電話番号等の情報を提供するが，商品のマーケティングのため等に利用する場合は，年齢しか提供しない等といったような定義がされていると，ユーザがカスタマサービスを提供してくれるような環境に入った際に，前もって許可されている情報は自動にサービス提供側に提供され，その情報をもとにユーザのカスタマカードが作成され，そのユーザに適したサービスが提供されることになるのである．

実際に，新しいサービスを受ける際には，どのような情報が必要とされているか，また何のために必要とされるかがわからないので，新しいサービスを受けられる範囲内に入った際にはそこで要求された個人情報についてすべてが通知の状況になるようにして，その場でユーザが定義を決め，再度同じサービスを受ける際には，前回定義したものを使えるようにすることになっている．

以下は，プリファレンスファイルの一部を示したものである．属性の behavior に定義してあるのが動作で，この場合は許可になっている．statement タグ内に定義されているのが実際の条件で，この場合，サービス提供を受けるために，サービス提供者だけがその個人情報を利用するという条件のものであったらユーザのロケーションと提供することを許可するという定義になっている．

```
<RULE behavior="accept">
 <POLICY>
  <STATEMENT>
   <PURPOSE><current></current></PURPOSE>
   <DATA ref="#user.location"></DATA>
   <RECIPIENT><ours></ours></RECIPIENT>
  </STATEMENT>
 </POLICY>
</RULE>
```

A.3　比較処理

実際に，この二つのファイルを比較して，要求された個人情報のうち提供できるものを判定し，提供された個人情報をもとにユーザに合わせたサービスを提供できる範囲で与えることになる．

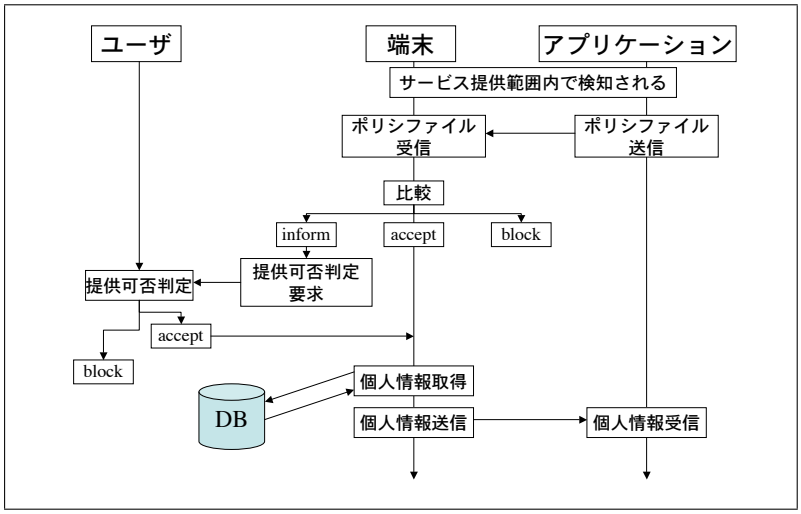

図 A.1: Penates 概要

比較の手順としては，ポリシファイルに定義されている statement を上から順に比較することになる．まず，何の個人情報が要求されているかをみて，例えばユーザ名であったらユーザに名について定義してある項目がプリファレンスファイルにあるかをプリファレンスファイルの上から順に探し，一致したら，その中の定義で利用目的や，利用期間等を比較し，お互いの定義が一致するものであったらその statement の属性の behavior から動作を取得し，accept ならその情報を提供することになる．この際，同一の項目についての定義がなかったり，利用目的等が一致しなかった場合は，すべて通知の項目になるものとされ，通知と判定された個人情報に関しては，図 A.1 に示されるようにその都度ユーザにその旨が通知される．通知される場合は，ポリシファイルの属性の description にあったようにその個人情報利用のための詳細説明が一緒に表示され，それをもとにユーザはその個人情報の提供の有無を判断することができる．そして，最終的に，比較が終わった時点で accept として判定された個人情報は全て，許可されている利用用途と共に，アプリケーション側に提供されることになる．そして，アプリケーション側では，その利用用途に従って，提供できるクオリティのサービスを提供することになる．

ここで注意しなければならないのは，サービス提供側に提供された個人情報の中に，必要不可欠なものが入っていなかったら何もサービスを提供することができない場合があるということである．このような場合には，足りていない個人情報を明記し，その情報がないと，提供できるサービスがないということをユーザに通知するようにしている．

付 録Ｂ　アンケート結果

1．よく行く店でポイントカードを作るかどうかを聞かれた時、
1-1．買い物ごとにポイントを貯めると一定ポイントが貯まった次点でサービス券を引き換えができることのみを伝えられた
1-1-1．カードを作りますか？
■ 作る　７３
□ 作らない　１９
1.1.2. 作ると答えた人へ
次に上げる情報のうち提供したくない情報はありますか？
■ 住所　４３
□ 氏名　４
□ 年齢　１０
□ 性別　２
□ 買い物頻度　１０
1-2．そこでも購入情報と、年齢・性別等を組み合わせて今後の商品入荷の傾向をとるための在庫管理に利用することを伝えられました
1-2-1 カードを作りますか？
■ 作る　６４
□ 作らない　２８
1-2-2 1-1-1 で作るにしたのに、今回作らないと答えた人へ
理由があったら書いてください
□ なぜですか？(理由があったら教えてください)

信用度による DM がいらない 自分にプラスにならない気がする 履歴は残したくない 面倒

2．よく行く百貨店でポイントカードを作ったと仮定してください。
そこで、カード作成のために提供した個人情報は以下の通りです。
＊ 住所
＊ 氏名
＊ 年齢
＊ 職業
2-1. 以下のリストの中で勝手に取得されていては嫌な情報はどれですか？
□ 入店時間　８
□ 退店時間　１２
□ 購入品目　１８

□ 店内の移動記録（どの経路を通って動いたか、どのフロアにどのくらい時間を使ったか等）４８
□ 決算方法（キャッシュかカードか等）　２７
2-1-1. 取得されて嫌な情報があった方は理由を教えてください

監視されている気がする 同じ傾向の商品ばかり勧められるのは嫌だ 必要性を感じない（移動記録） プライバシ侵害 購入価格によってランク付けされてる気がする

3．ポイントカードやカスタマーカードと言われるようなカードを作成する際、常に本当の情報を提供しますか？
■ はい　７７
□ いいえ　１５
3-1. いいえと答えた方へ
どのようなときに嘘の情報を提供しますか？

生年月日や電話番号 人的管理がされている店 年収や仕事内容 趣味嗜好

3-2. はいと答えた方へ
カード作成後、または作成前にカードについて書かれた資料をもらうと思いますが、そこに書かれた個人情報取り扱いに関する情報を目に通しますか？
□ 必ず読む　１８
□ たまに読む　５５
■ 読まない　１９
4. ポイントカード等を作るかどうか聞かれた際、それを作るかどうかは何を判断基準としていますか？(例、店の名前、利用頻度、カードの特典内容、等)

気分、よく使う店か 利用頻度・特典内容 有効期限 店のブランド 店の評判 商品の充実性 クレジットカードでない事

5. 現在（電子的な紙じゃないもの）ポイントカード等を持っている人へ
そのポイントカードが、店側に取ってポイントを貯める意外の目的があるかもしれないと考えたことがありますか？もしくはあると認識していますか？
■ はい　３８
□ いいえ　５４

付 録C　個人情報保護法案

C.1　総則：第一章

C.1.1　目的：第一条

個人情報の有用性に配慮しつつ，個人の権利利益を保護する

C.1.2　定義：第二条

個人情報とは，生存する個人に関する情報であり，それにより特定の個人を識別することができるものである

- 個人データベース
  - 特定の個人情報を電子計算機を用いて検索することができるように構成したもの
  - このデータベースを事業用として用いているものを個人情報取り扱い事業者と呼ぶ
  - このデータベースを構成する個人情報を個人データと呼ぶ
- 保有個人データ
  - 個人情報取り扱い事業者が開示，内容の訂正，追加または削除，利用の停止，消去および第三者への提供の停止をおこなうことのできる権限を有する個人データ

C.2　基本原則：第二章

C.2.1　利用目的による制限：第四条

個人情報はその利用の目的が明確にされるとともに，当該目的の達成に必要な範囲内で取り扱わなければならない

C.2.2　適正な取得：第五条

個人情報は適法かつ適正な方法で取得されなければならない

C.2.3　正確性の確保：第六条

個人情報はその利用の目的に達成に必要な範囲内で正確かつ最新の内容に保たなければならない

C.2.4　安全性の確保：第七条

個人情報の取り扱いに関して，漏えい，滅失またはき損の防止その他の安全管理のため必要かつ適切に取り扱われるよう配慮されなければならない

C.2.5　透明性の確保：第八条

個人情報の取り扱いに当たっては，本人が適切に関与しえるよう配慮されなければならない

C.3　国及び地方公共団体の責務等：第三章

C.3.1　国の責務：第九条

国はこの法律の趣旨にのっとり，個人情報の適正な取り扱いの確保するために必要な施策を総合的に策定し，及びこれを実施する責務を有する

C.3.2　地方公共団体の責務：第十条

地方公共団体はこの法律の趣旨にのっとり，その地方公共団体の区域の特性に応じて，個人情報の適正な取り扱いを確保するために必要な施策を策定し，及びこれを実施する責務を有する

C.3.3　法制上の措置等：第十一条

政府は国の行政機関について，その保有する個人情報の適正な取り扱いが確保されるようにする

C.4　個人情報の保護に関する施策等：第四章

C.4.1　個人情報の保護に関する基本方針：第一節

政府は個人情報の保護に関する施策の総合的かつ一体的な推進を図るため，個人情報の保護に関する基本方針を定めなければならない：第十二条

C.4.2　国の施策：第二節

- 地方公共団体への支援：第十三条
  国は地方公共団体が策定し，または実施する個人情報の保護に関する施策及び国民または事業者等が個人譲歩の適正な取り扱いの確保に関しておこなう活動を支援するため，情報の提供，事業者等が講ずべき措置の適切かつ有効な実施を図るための指針の策定その他の必要な措置を講ずる

- 苦情処理のための措置：第十四条
  国は個人情報の取り扱いに関し事業者と本人との間に生じた苦情の適切かつ迅

速な処理を図るために必要な措置を講ずる

- 個人情報の適正な取り扱いを確保するための措置：第十五条国は地方公共団体との適切な役割分担を通じ，個人情報取り扱い事業者による個人情報の適正な土地扱いを確保するために必要な措置を講ずる

C.4.3　地方公共団体の施策：第三節

- 保有する個人情報の保護：第十六条当団体は，保有する個人情報の性質，当該個人情報を保有する目的等を把握し，その保有する個人情報の適正な取り扱いが確保されるよう必要な措置を講ずる
- 区域内の事業者等への支援：第十七条当団体は，個人情報の適正な取り扱いを確保するため，その区域内の事業者及び住民に対する支援に必要な措置を講ずる
- 苦情処理のあっせん等：第十八条当団体は，個人情報の取り扱いに関し事業者と本人との間に生じた苦情が適切かつ迅速に処置されるようにするため，苦情処理のあっせんその他必要な措置を講ずる

C.4.4　国及び地方公共団体の協力：第四節

- 国及び地方公共団体は，相協力する：第十九条

C.5　個人情報取り扱い事業者の義務等：第五章

C.5.1　個人情報取り扱い事業者の義務：第一節

- 利用目的の特定：第二十条個人情報取り扱い事業者は，個人情報を取り扱うにあたっては，その利用目的をできる限り特定すべきである
  - これを変更する場合には，変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えておこなってはならない
- 利用目的による制限：第二十一条
  - 個人情報取り扱い事業者は，本人の同意を得ないで，既存に規定された利用目的の達成に必要な範囲を超えて個人情報を取り扱ってはならない
  - 個人情報取り扱い事業者は，合併その他の理由によりほかの個人情報事業者から事業を継承することに伴って個人情報を取得した場合は，あらかじめ本人の同意を得ずに継承前における利用目的の達成に必要な範囲を超えて当該個人情報を取り扱ってはならない
  - 適用外
    - 法令に基づく場合
    - 人の生命，身体または財産の保護のために必要がある場合であって，本人の同意を得ることが困難であるとき
    - 公衆衛生の向上または児童の健全な育成の推進のために特に必要がある場合であって，本人の同意を得ることが困難であるとき

        * 国の機関，地方公共団体またはその委託を受けたものが法令の定める事務を遂行することに対し協力する必要がある場合であって，本人の同意を得ることにより当該事務の遂行に支障を及ぼす恐れがあるとき

- 適正な取得：第二十二条個人情報取り扱い事業者は，偽りその他不正な手段により個人情報を取得してはならない

- 取得の際の利用目的の通知等：第二十三条

    - 個人情報を取得した場合は，あらかじめその利用目的を公表している場合を除き，速やかにその利用目的を本人に通知，または公表しなければならない
    - 利用目的の変更の際には，本人に通知または公表しなければならない
    - 適用外
        * 利用目的の通知，または公表により本人または第三者の生命，身体，財産その他の権利利益を害する恐れがある場合
        * 通知または公表により当該個人情報取り扱い事業者の権利または正当な利害を害する恐れがある場合
        * 国の機関または地方公共団体は法令の定める事務を遂行することに対して協力する必要がある場合であり，利用目的を本人に通知または公表することにより当該事務の遂行に支障を及ぼす恐れがあるとき
        * 取得の状況から見て利用目的が明らかであると認められる場合

- データ内容の正確性の確保：第二十四条個人情報取り扱い事業者は，利用目的の達成に必要な範囲において，個人データを性格かつ最新の内容に保つよう努めなければならない

- 安全管理措置：第二十五条事業者は，取り扱う個人データの漏えい，滅失またはき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じる

- 従業者の監督：第二十六条事業者は，個人データを従業員に取り扱わせるにあたって，当該個人データの安全管理が図られるよう，当該従業者に対する必要かつ適切な監督をおこなわなければならない

- 委託先の監督：第二十七条事業者は，個人データの取り扱いの一部または全部をほかの事業に委託する際，その事業に対する必要かつ適切な監督をおこなわなければならない

- 第三者提供の制限：第二十八条事業者は基本的に本人の同意を得ずに個人データを第三者に提供してはならない

- 適用外第二十一条の適用外例と同様プラス

    - 個人情報取り扱い事業者は，第三者に提供される個人データについて，本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止することとしている場合であり，次に挙げる事項について，あらかじめ，本人に通知，または本人が容易に知りえる状態においているときは，当該個人データを第三者に提供することが可能

        * 第三者への提供を利用目的とする
        * 第三者に提供される個人データの項目
        * 第三者への提供の手段または方法
        * 本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止する
    - 第三者に該当しない場合
        * 個人データの取り扱いについて全部または一部を利用目的の達成に必要な範囲内で委託される場合
        * 合併その他の理由により事業の継承に伴って個人データが提供される場合
        * 個人データを特定の者との間で共同して利用する場合であり，その旨並びに共同して利用される個人データの項目，共同して利用する者の範囲，利用する者の利用目的及び当該個人データの管理について責任を有する者の氏名または名称について，あらかじめ本人が把握している場合
    - 事業者は第三者が規定する利用目的または個人データの管理について責任を有する者の情報などに変更が生じた際に，あらかじめ本人が把握できるようにすべきである

- 保有個人データに関する事項の公表等：第二十九条
    - 事業者は，保有個人データ関し，次に挙げる事項について，本人の知りえる状態に置くべきである
        * 当該事業者の氏名または名称
        * すべての保有個人データの利用目的
        * 保有個人データの適正な取り扱いの確保に関して必要な事項として政令で定めるもの
    - 事業者は，本人から当該本人が識別される保有個人データの利用目的の通知を求められたときは，利用目的が明らかに掲示されている場合等を除き，本人に対し，遅滞なく，これを通知しなければならない
    - 事業者は，個人データの利用目的を通知しない旨を決定した際，本人に対し，遅滞なく，その旨を通知しなければならない

- 開示：第三十条事業者は，本人から，当該本人が識別される保有個人データの開示を求められたとき，以下の例外を除いて，本人に対し，政令で定める方法により，遅滞なく，当該保有個人データを開示しなければならない
    - 本人または第三者の生命，身体，財産その他の権利利用を害する恐れがある場合
    - 当該個人情報取り扱い事業者の義務に適正な実施に著しい支障を及ぼす恐れがある場合
    - 他の法令に違反することとなる場合

  これについて開示しない旨を決定した際は，本人に対し，遅滞なく，その旨を通知しなければならない

- 訂正等：第三十一条
  - 事業者は本人から，当該本人が識別される保有個人データの内容が事実でないという理由によって当該保有個人データの内容の訂正，追加または削除を求められた場合には，その内容の訂正等に関して他の法令の規定により特別の手続きが定められている場合を除き，利用目的の達成に必要な範囲内において，遅滞なく必要な調査をおこない，その結果に基づき，当該保有個人データの内容の訂正等をおこなわなければならない
  - 事業者は，前項の規定に基づき求められた個人データの内容の全部または一部について訂正等をおこなったとき，また訂正等をおこなわない旨の決定をした際には，本人に対し敏速にその旨を通知しなければならない
- 利用停止等：第三十二条
  - 事業者は，本人から，当該本人が識別される保有個人データが第二十一条の規定に違反して取り扱われているという理由または第二十二条の規定に違反して取得されたものであるという理由によって，当該保有個人データの停止または消去を求められた場合であって，その求めに理由があることが判明したときは，違反を是正するために必要な限度で，遅滞なく，当該保有個人データの利用停止等をおこなわなければならない
  - しかし，当該保有個人データの利用停止等に多額の費用を要する場合その他の利用停止等をおこなうことが困難な場合であって，本人の権利利益を保護するため必要なこれに変わるべき措置をとるときはこの限りではない
  - 事業者は，本人から，当該本人が識別される保有個人データが第二十八条の規定に違反して，第三者に提供されているという理由に同データの第三者への提供の停止を求められた場合であって，その求めに理由があることが判明したときは，遅滞なく，同データの提供を停止ししなければならない
  - これに関しても，停止に多額の費用を要する場合その他の第三者への提供を停止することが困難な場合であって，代わりの措置をとるときはこの限りではない
  - 事業者は規定に基づき求められた個人データの全部もしくは一部について利用停止等をおこなった場合，また，停止をおこなわない旨の決定をした際，その旨を本人に対し遅滞なく通視しなければならない
- 理由の説明：第三十三条前項規定により，本人から求められた措置の全部または一部について，その措置をとらない旨を通知する際，または求められた措置と異なる措置をとる旨を通知する場合には，本人に対し，その理由を説明するよう努めなければならない
- 開示等の求めに応じる手続き：第三十四条
  - 事業者は示等の求めに関し，政令で定めるところにより，その求めを受け付ける方法を定めることができる
    - この場合，本人は当該方法に従って，開示等の求めをおこなわなければならない

  - 事業者は，本人に対し，開示等の求めに関し，その対象となる保有個人データを特定するに足りる事項の提示を求めることができる
    * この場合，事業者は，本人が容易且つ明確開示等の求めをすることができるよう，当該保有個人データの特定に資する情報の提供その他本人の利便を考慮した適切な措置をとらなければならない
  - 開示等の求めは，政令で定めるところにより，代理人によってすることができる
  - 事業者は規定に基づき開示等の求めに応じる手続きを定めるに当たっては，本人に過重な負担を課するものとならないよう配慮しなければならない
- 手数料：第三十五条
  - 事業者は，第二十九条の規定による利用目的の通知または第三十条による開示を求められたときは，当該措置の実施に関し手数料を徴収することができる
  - 前項規定により手数料を徴収する場合は，実費を勘案して合理的であると認められる範囲内において，その手数料の額を定めなければならない
- 個人情報取り扱い事業者による苦情の処理：第三十六条
  - 事業者は，個人情報の取り扱いに関する苦情の適切かつ迅速な処理に努めなければならない
  - 前項の目的を達成するために必要な体制の整備に努めなければならない
- 報告の徴収：第三十七条主務大臣は，この節の規定の施行に必要な限度において，個人情報取り扱い事業者に対し，個人情報の取り扱いに関し報告させることができる
- 助言：第三十八条主務大臣は，この節の規定の施行に必要な限度において，個人情報取り扱い事業者に対し，個人情報の取り扱いに関し必要な助言をすることができる
- 勧告及び命令：第三十九条
  - 主務大臣は，事業者が第二十一条から第二十三条まで，第二十五条から第三十二条までまたは，第三十五条の規定に違反した場合において個人の権利利益を保護するために必要があると認めるときは，当該個人情報取り扱い事業者に対し，当該違反行為の中止その他違反を是正するために必要な措置をとるべき旨を勧告することができる
  - 主務大臣は，前項規定による勧告を受けた事業者が正当な理由がなくその勧告に係る措置をとらなかった場合において，個人の重大な権利利益の侵害が切迫していると認めるときは，事業者に対しその勧告に係る措置をとるべきことを命ずることができる
  - 前二項の規定にかかわらず，事業者が第二十一条，二十二条，二十五条から七条，二十八条の規定に違反した場合において，個人の重大な権利利益を害する事実があるため緊急に措置をとる必要があると認めるときは，事業者に対し，当該違反行為の中止その他違反を是正するために必要な措置をとるべきことを命ずることができる

- 配慮義務：第四十条主務大臣は前三条の規定により事業者に対し，報告の徴収，助言，勧告または命令をおこなう場合においては，表現の自由，学問の自由，信教の自由及び政治活動の自由を妨げることがないよう配慮しなければならない
- 主務大臣：第四十一条
  - 内閣総理大臣は，この説の規定の円滑な実施のため必要があると認める場合には，個人情報取り扱い事業者がおこなう個人情報の取り扱いのうち特定のものについて，特定の大臣または国家公安委員会を主務大臣に指定することができる
  - その他でこの節における主務大臣は次の通りとする
    - 事業者がおこなう個人情報の取り扱いのうち雇用管理に関するものについては，厚生労働大臣 (船員の雇用管理に関するものについては，国土交通大臣) 及び当該個人情報取り扱い事業者がおこなう事業を所管する大臣等
  - 内閣総理大臣は前項但し書きの規定により主務大臣を指定したときは，その旨を公示しなければならない
  - 各主務大臣は，この節の規定の施行に当たっては，相互に緊密に連絡し，及び協力しなければならない

C.5.2 民間団体による個人情報の保護の推進：第二節

- 認定：第四十二条
  - 事業者の個人情報の適正な取り扱いの確保を目的として，次の各号に挙げる業務をおこなおうとする法人は，主務大臣の認定を受けることができる
    - 業務の対象となる事業者の個人情報の取り扱いに関する第四十七条の規定による苦情の処理
    - 個人情報の適正な取り扱いの確保に寄与する事項についての対象事業者に対する情報の提供
    - 他，対象事業者の個人情報の適正な取り扱い確保に関し必要な業務
  - 認定を受けようとするものは，政令で定めるところにより，主務大臣に申請しなければならない
  - 主務大臣は，認定をおこなった際にはその旨を公示しなければならない
- 欠格条項：第四十三条いずれかに該当するものは，前条の認定を受けることができない
  - この法律の規定により刑に処せられ，その執行を終わり，または執行を受けることがなくなった日から二年を経過しない者
  - 第五十三条の規定により認定を取り消され，その取り消しの日から二年を経過しない者
  - その業務をおこなう役人のうち，次のいずれかに該当する者があるもの

    - 禁固以上の刑に処せられ，またはこの法律の規定により刑に処せられ，その執行を終わり，または執行を受けることがなくなった日から二年を経過しない者
    - 第五十三条の規定により認定を取り消された法人において，その取り消しの日前 30 日以内にその役員であったものでその取り消しの日から二年を経過しない者

- 認定の基準：第四十四条主務大臣は，第四十二条の認定の申請が次の各号のいずれにも適合していると認めるときでなければ，その認定をしてはならない
    - 第四十二条に揚げる業務を適性かつ確実におこなうに必要な業務の実施の方法が定められているものであること
    - 第四十二条に揚げる業務を適性かつ確実におこなうに足りる知識及びその能力ならびに経済的基礎を有するものであること
    - 第四十二条にあげる業務以外の業務をおこなっている場合には，その業務をおこなうことによって，同項各号に揚げる業務が不公正になる恐れがないものであること

- 廃止の届出：第四十五条
    - 第四十二条の認定を受けたものは，その認定に係る業務を廃止しようとするときは，政令で定めるところにより，あらかじめ，その旨を主務大臣に届け出なければならない
    - 主務大臣は，前項の規定による届出があったときは，その旨を公示しなければならない

- 対象事業者：第四十六条
    - 認定個人情報保護団体は，当該認定個人情報保護団体の構成員である個人情報取り扱い事業者または認定業務の対象となることについて同意を得た事業者を対象事業者としなければならない
    - 認定個人情報保護団体は，対象事業者の氏名または名称を公表しなければならない

- 苦情の処理：第四十七条
    - 保護団体は，本人等から対象事業者の個人情報の取り扱いに関する苦情について解決の申し出があったときは，その相談に応じ，申し出人に必要な助言をし，その苦情に係る事情を調査するとともに，当該対象事業者に対し，その苦情の内容を通知してその迅速な解決を求めなければならない
    - 保護団体は，前項の申し出に係る苦情の解決について必要があると認めるときは，当該対象事業者に対し，文書もしくは口頭による説明を求め，または資料の提出を求めることができる
    - 対象事業者は，保護団体からの前項の規定による求めがあったときは，正当な理由がないのに，これを拒んではならない

- 個人情報保護指針：第四十八条

  - 保護団体は，対象事業者の個人情報の適正な取り扱いの確保のために，利用目的の特定，安全管理のための措置，本人の求めの応じる手続きその他の事項に関し，この法律の規定に沿った指針を作成し，公表するよう努めなければならない (個人情報保護指針)
  - 当団体は，前項の規定により保護指針を公表したときは，対象事業者に対し，それを守らせるため必要な指導勧告その他の措置をとるよう努めなければならない

- 目的外利用の禁止：第四十九条保護団体は，認定業務の実施に際して知り得た情報を認定業務の用に供する目的以外に利用してはならない
- 名称の使用制限：第五十条保護団体ではないものは，認定個人情報保護団体という名称またはこれに紛らわしい名称を用いてはならない
- 報告の徴収：第五十一条主務大臣は，この節の規定の施行に必要な限度において，保護団体に対し，認定業務に関し報告をさせることができる
- 命令：第五十二条主務大臣は，この節の規定の施行に必要な限度において，保護団体に対し，認定業務の実施の方法の改善，保護指針の変更その他の必要な措置をとるべき旨を命ずることができる
- 認定の取り消し：第五十三条
  - 主務大臣は，保護団体は次のいずれかに該当するときはその認定を取り消すことができる
    - 第四十三条の規定に該当するに至ったとき
    - 四十四条のいずれかに適合しなくなったとき
    - 四十九条の規定に違反したとき
    - 前条の命令に従わないとき
    - 不正手段により認定を受けたとき
  - 主務大臣は，前項の規定により認定を取り消したときは，その旨を公示しなければならない
- 主務大臣：第五十四条
  - 設立について許可または認可を受けている認定個人情報保護団体については，その設立の許可または認可をした大臣等
  - 他，保護団体の対象事業者がおこなう事業を管轄する大臣等
  - 前述と同様，内閣総理大臣は必要があると認める場合は特定の大臣等を指定することができる
    - 特別に指定した際には，その旨を公示しなければならない

C.6 雑則：第六章

C.6.1 適用除外：第五十五条

- 事業者のうち次に揚げるものについては前章の規定は適用しない

  - 放送期間，新聞社，通信社その他の報道機関報道の用に供する目的
  - 大学その他の学術研究を目的とする機関もしくは団体またはそれらに属する者学術研究のように供する目的
  - 宗教団体宗教活動の用に供する目的
  - 政治団体政治活動の用に供する目的
- 前項に揚げる事業者は個人データの安全管理のために必要かつ適切な措置，個人情報の取り扱いに関する苦情の処理その他の個人情報の席聖な取り扱いを確保するために必要な措置を自ら講じ，かつ当該措置の内容を公表するよう努めなければならない

C.6.2　地方公共団体が処理する事務：第五十六条

この法律に規定する主務大臣の権限に属する事務は，政令で定めるところにより，地方公共団体の長その他の執行機関がおこなうこととすることができる

C.6.3　権限または事務の委任：第五十七条

この法律により主務大臣の権限または事務に属する事項は，政令で定めるところにより，その所属の職員に委任することができる

C.6.4　施行の状況の公表：第五十八条

- 内閣総理大臣は，関係する行政機関及び内閣の所轄の下に置かれる機関，内閣府，宮内庁，内閣府設置法に規定する機関ならびに国家行政組織法の長に対し，その法律の施行の状況について報告を求めることができる
- 内閣総理大臣は毎年度，前項の報告を取りまとめ，その概要を興行するものとする

C.6.5　連絡及び協力：第五十九条

内閣総理大臣及びこの法律の施行に関係する行政機関の長は，相互に緊密に連絡し，及び協力しなければならない

C.6.6　政令への委任：第六十条

この法律に定めるものの他，この法律の実施のため必要な事項は，政令で定める

C.7　罰則：第七章

C.7.1　第六十一条

第三十九条のきれいによる命令に違反したものは六ヶ月以下の懲役または三十万円以下の罰金に処する

C.7.2　第六十二条

第三十七条または五十一条の規定による報告をせず，または虚偽の報告をしたものは三十万円以下の罰金に処する

C.7.3　第六十三条

- 法人の代表者または法人もしくは人の代理人，使用人その他の従業者が，その法人または人の業務に関して，前二条の違反行為をしたときは，行為者を罰するほか，その法人または人に対しても各本条の罰金刑を科する
- 法人でない団体について前項の規定の適用がある場合には，その代表者または管理人が，その訴訟行為につき法人でない団体を代表するほか，法人を被告人または被疑者とする場合の刑事訴訟に関する法律の規定を準用する

C.7.4　第六十四条

次のいずれかに該当するものは，１０万円以下の過料に処する

- 第四十五条の規定による届出をせず，また虚偽の届出をした者
- 第五十条の規定に違反して者

C.8　附則

C.8.1　施行期間：第一条

- この法律は公布の日から施行する
- 第五章から七章まで及び附則二条から六条までの規定は公布の日から起算して二年を超えない範囲内において政令で定める日から施行する

C.8.2　本人の同意に関する経過措置：第二条

この法律の施行前になされた本人の個人情報の取り扱いに関する同意がある場合において，その同意が第二十条の規定により特定される利用目的以外の目的で個人情報を取り扱うことを認める旨の同意に相当するものであるときは，第二十一条の同意があったものとみなす

C.8.3　第三条

法律施行前になされた本人の個人情報の取り扱いに関する同意がある場合において，その同意が第二十八条の規定による個人データの第三者への提供を認める旨の同意に相当するものであるときは，動向の同意があったものとみなす

C.8.4　通知に関する経過措置：第四条

第二十八条の規定により本人に通知し，または本人が容易に知りえる状態に置かなければならない事項について，この法律の施行前に本人に通知されているときは同項の規定により定められたものとする

C.8.5　名称の利用制限に関する経過措置：第六条

この法律の施行の際，現に認定個人情報保護団体という名称またはこれに紛らわしい名称を用いているものについては第五十条の規定は同条規定の施工後六ヶ月は適用しない

C.8.6　法制上の措置：第七条

政府はこの法律の公布後一年を目途として，第十一条に規定する法律上の措置を講ずる

C.8.7　内閣府設置法の一部改正：第八条

高度情報通信社会の進展に伴い個人情報の利用が著しく拡大していることにかんがみ，個人情報の有用性に配慮しつつ，個人の権利利益を保護するため，個人情報の適正な取り扱いに関し，基本原則及び政府による基本方針の作成その他の個人情報の保護に関する施策の基本となる事項を定め，国及び地方公共団体の責務等を明らかにするとともに，個人情報と取り扱う事業者の守るべき義務等を定める必要が出たため

付 録D　名誉毀損罪

名誉毀損罪とは，民事と刑事のにタイプがある．民事は，原則として客観的な社会評価が保護されるためのものである．単なる主観的名誉感情の損害は含まれない．また，刑事における名誉毀損罪とは，公然と事実を摘示し，人の名誉を毀損した場合に成立する．この際，事実の有無，真偽を問わないが，公共の利害に関する事実に関係する事を，専ら公益目的で摘示した結果，名誉を毀損するに至った場合には，その事実が真実である場合は処罰されないことになっている．

実際にあった例を挙げて説明すると，名誉を毀損する表現であっても，以下のような要件がそろったら処罰されず，損害賠償を支払わなくてもいいということもあるらしい．

- 公共の利害に関する事実にかかるないようであって（公共性）
- 表現行為の目的が専ら公益を図るものであり（公益性）
- 当該事実が真実である事が証明されるか（真実性）
- 行為者がそれを真実であると過信した事について相当の理由がある（相当性）

付 録E　プロバイダ責任制限法

E.1　プロバイダが賠償の責を負わずにすむ場合

プロバイダは，情報送信者と情報ユーザの間で仲介している事から，送信された内容が第三者の権利を侵害する者であったりした場合，責任を追及される事が多い．しかし，プロバイダの果たす役割は大きい上に，表現の自由と，プライバシの侵害・信用侵害等の問題が同時に存在する状況なので，ある一定の手順を踏んでいればプロバイダに責任が講じないようにするため定められた．

E.1.1　情報によって権利を侵害されたとする被害者からの追求に対して

プロバイダが送信を許可している情報によって，権利が侵害されたとしてプロバイダ側に責任が追及されたとき，以下の例外を除いて，賠償の責めに任じられない．

- 情報の流通によって，他人の権利が侵害されていることを知っていた場合
- 情報の流通によって，他人の権利が侵害されていることを知ることができたと認めるに足りる相当の理由があったとき

E.1.2　情報送信者からの追求に対して

送信している情報に関して，送信防止措置を講じた際，表現の自由などによって情報送信者から権利侵害で賠償責任を求められた際，次のいずれかに該当する場合，賠償の責めに任じられない．

- 送信情報が，他人の権利を侵害されていると信じるに足りる相当の理由があった場合
- 権利侵害によって，情報送信防止措置を要求する申出が合った場合で，その旨を送信者に通知し，措置に同意するかどうか照会した場合において，七日以内に反論がなかった場合

E.2　権利を侵害された者が，送信者に関する情報の開示を請求することができる条件

送信されている情報によって，自分の権利が侵害されていると思われる際，以下の条件の基で情報送信者に関する情報の開示を請求することができる

- 侵害情報の流通によって，その者の権利が侵害されたことが明らかである場合
- その情報が，損害賠償請求権の行使のために必要である場合等，開示を受けるべき正当な理由がある場合

E.3　その他の規約

- 前述した規定に基づいた情報開示請求を受けた場合，その旨を開示される本人に伝えなくてはならない
- 情報開示請求によって，情報を入手した者は，その情報をみだりに利用したり，情報者本人の生活の平穏を乱すようなことをしてはならない

付 録F　プロバイダ規制ガイドライン

上記のプロバイダ制限法で守られるために取るべき手順を記したガイドラインである.

F.1　ガイドラインの目的及び範囲

F.1.1　ガイドラインの目的

このガイドラインのは，特定電気通信役務提供者（以下プロバイダ）の損害賠償責任の制限及び発信者情報の開示に関する法律を踏まえて，プロバイダによる情報の流通により名誉を毀損され，またはプライバシを侵害された申立者からの送信防止措置の要請を受けた場合にプロバイダの取るべき行動基準を明瞭化することにより，申立者，発信者及びプロバイダ等それぞれの関係者の利益を尊重しつつ，プロバイダ等による迅速かつ適切な対応を促進し，もってインターネットの円滑かつ健全な利用を促進することを目的とする

F.1.2　ガイドラインの判断基準の位置付け

このガイドラインは以下のような点に重点を置いて記されている.

- 送信防止措置を講じなかったとしても，被害者に対する損害賠償責任を負わないケースにはどのような物があるか
- 被害者当からの要請に応じて送信防止措置を講じた場合に，発信者に対する損害賠償責任を負わないケースにはどのような物があるか

また，プロバイダ等の損害賠償責任が制限されるかどうかは，最終的には裁判所によって決定されるものであるので，このガイドラインに従って対応しなければ常に損害賠償責任が生じるとは限らないし，逆にこのガイドラインに従って対応していても責任が生じることはある．これは，あくまでも名誉毀損及びプライバシ侵害に該当する情報に自立的に対応する独自の判断基準を整備することを可能にするための手助けのための活用されることを念頭に作成されたものである.

さらに，このガイドラインは今後社会環境の変容に伴って起こる名誉やプライバシに関する意識の変化，情報技術の発展及び実務の運用状況において常に変わっていくものである.

F.1.3　ガイドラインの適用対象外となるもの

プロバイダ責任制限法で規定されていない事項については原則として取り扱わない.例えば，電子メールによる名誉毀損等である．このガイドラインでは，ネットでのウェ

ブページや電子掲示版等のように不特定のものに対して情報を送信する形態でおこなわれる電気通信における場合のみである．

F.1.4　プロバイダ責任制限法の考え方

- 申立者に対する損害賠償責任の制限
  個人相手にプロバイダ等が送信防止措置の要請を受ける情報としては，プライバシ侵害，侮辱，肖像権侵害等があり，法人相手では，信用毀損，業務妨害等に相当する情報が考えられる．これらの情報について，削除等の送信防止措置を講じるよう申し出を受けた場合，プロバイダ等の責任が問われる可能性がある．

  しかし，プロバイダ等には，自己管理下にあるサーバに格納された情報が他人の権利を侵害していないかどうかを監視する義務はない．これは表現の自由に対する萎縮効果をもたらす可能性があるからである．

  また，申立者からの送信防止措置の要請等を契機として，ウェブページや掲示板に掲載された情報の流通をプロバイダが知ったときは，送信防止措置を講じなかったとしても，これによって「他人の権利が侵害されていることを知ることができたと認めるに足りる相当の理由」がなければ，プロバイダ等は申立者との関係で当該情報を放置したことによる責任は負わない．

  さらに，送信防止措置を講じることが技術的に不可能な場合にはそもそもプロバイダ等にこれを期待することはできないので責任は負わないこととなる．

- 発信者に対する損害賠償責任の制限
  実際に送信防止措置の要請を受けたサイトが，名誉毀損やプライバシ侵害に当たるような表現をしているかどうかを判断するのは非常に難しい．同じ表現であってもときと場合によって名誉毀損に当たる場合もあれば当たらない場合もある．このような状況の中で，プロバイダ等が間違って判断し，削除してしまったときには，発信者から損害賠償を請求される可能性があるのである．これは，プロバイダ等が送信防止措置をおこなうことを避ける傾向を呼んでしまうので，プロバイダ責任制限法はある一定の条件下ではプロバイダ等が発信者に対する損害賠償責任を負わないことを定めている．

  1. 不当な権利侵害がおこなわれたと信じるに足りる相当の理由があった場合
  2. 発信者に送信防止措置に同意するかどうかの紹介手続きをおこなった日から七日以内に反論の申し出がない場合
  3. 名誉毀損等の書き込みがなされたウェブページに送信防止措置を講じるのに必要最低限の措置を講じた場合

F.2　送信防止措置の判断基準

F.2.1　総論

- 法務省人権擁護機関からの削除依頼への対応
  前に記述した要領で，法務省人権擁護機関からの要請を受けたことによってプロバイダ等が情報の削除をおこなった場合,「他人の権利が不当に侵害されてい

ると信じるに足りる相当な理由がある」場合に該当し，発信者からの損害賠償責任を負わない場合が多い．

- プロバイダ等の行動指針としての判断基準
  ガイドラインに法的効力はないが，削除等の依頼があったにもかかわらず，情報について送信防止措置を講じることなく放置した場合は，申立者との関係において「他人の権利が侵害されていることを知ることができたと認めるに足りる相当の理由がある」場合に該当する場合があるので注意が必要である．

F.2.2 個人の権利を侵害する情報の送信防止措置

- プライバシ侵害の観点からの対応
  - 一般私人の場合の削除対象
    - 氏名及び勤務先・自宅の住所・電話番号が掲載されたウェブページ
    - ネット上でハンドルネームのみで行動している場合に氏名を開示する情報が記載された場合
    - 公表されていない電子メールアドレスを開示する情報が記載された場合
  - 公人等について（国会議員，都道府県の長，議員その他要職に就く公務員）
    - 氏名，勤務先等の連絡場所の住所・電話番号等広く知られているものについては削除の必要がない
    - 職務と関係のない連絡先情報で広く知られる必要性のない情報は一般私人の場合と同様

  なお，電話番号として記載されたものが誤っていて別人物の電話番号が記載されている場合は，プライバシ侵害ではなく迷惑行為として削除対象となる．

  - 氏名・連絡先以外の個人情報
    - 一般私人について
      氏名・連絡先以外の情報に関しても，当該情報に含まれる記述等により特定の個人を識別できる場合，本人から削除要求があれば，発信者に対してその旨を伝え，自主的削除に応じない場合，プロバイダ等が削除可能な場合は原則として削除
    - 公人等について
      「職業上の事実」と言える場合等，削除しないでよい場合があるが,「私生活上の事実」に関しては一般私人と同じ扱いである
    - 犯罪関係者について
      被害者及びその関係者については，犯罪事実及びこれを密接に関連する事実については，削除要望があれば，発信者にその旨を伝え，自主的削除しない場合は，削除要請者に経過を伝え，自主的な解決を促すただし，その記載が品位を欠き目に余るとき等はプロバイダ等において削除可能なときもある
  - 写真，肖像等が掲載されたウェブページ等

* 被写体本人が識別可能な顔写真等の場合，写真の内容，掲載の状況からみて，本人の同意を得て撮影されてものではないことが明白な写真については，原則として削除可能だが，次の例外を除く
  - 行楽地等の雰囲気を出すために，群像として撮影された写真の一部に写ってるに過ぎず，特定の本人を大写しにしたものでない場合
  - 犯罪報道における被害者の写真等，実名及び顔写真を掲載することが公共の利害に関し，公益を図る目的である場合
  - 公人の職務に関する事柄など，社会の正当な関心ごとということのできる場合であり，顔写真掲載の手段方法が相当である場合
  - 著名人の顔写真については，当該著名人のパブリシティによる顧客吸引力を不当に利用しようとしたものでなく，社会の正当な関心ごとということのできる場合でその方法が相当である場合

  また，撮影それ自体について同意が得られていると思われる写真であっても，客観的にみて，通常の羞恥心を有する個人が公表されることに不快感または精神的苦痛を感じると思われる写真については削除できる場合が多い

F.2.3 名誉毀損の観点からの対応

特定個人の社会的評価を低下させる誹謗中傷の情報がウェブページ等に掲載された場合には，当該情報を削除できる場合があるが，以下の三つの要件を満たす可能性がある場合には，削除をおこなわない.

- 当該情報が公共の利害に関する事実であること
- 当該情報の掲載が個人攻撃の目的等ではなく公益を図る目的に出たものであること
- 当該情報が真実であるか，または発信者が真実と信じるに足りる相当の理由があること

しかし，特定個人に関する論評について，その域を超えて人身攻撃に及ぶような侮辱的な表現が用いられている場合は削除できる

F.2.4 企業その他法人の権利を侵害する情報の送信防止措置

企業その他の法人の名誉または信用を毀損する表現行為がおこなわれた場合，以下の理由からプロバイダ等において権利侵害の不当性について信じるに足りる理由がそろわないことがほとんどである．従って，プロバイダ責任制限法より，紹介手続き等を経て対応するのが妥当である.

しかし，その情報が与える影響が当該企業やその顧客に経済的に多大な損失を被らせるような圧迫した危険がある場合等，削除が認められる場合もある.

- 企業その他の団体がほとんどの場合，公的存在とみられること
- 表現行為が公共の利益に関する事実に係り専らかどうかは別としてそれなりに公益を図る目的でなされたと評価できること

- 表現が企業その他の団体の社会的評価を低下させても，そこで摘示された事実の真偽については，プロバイダ等において判断ができない場合が多いこと

F.3　送信防止措置を講じるための対応手順

F.3.1　申立の受付

プロバイダ責任制限法に基づく送信防止措置を講ずることの申出または発信者情報の開示に関する請求を受けることを想定して，苦情・相談窓口を設置し，自己の契約者以外のものからの申出に対しても迅速に対応でき手続きを開始するためには，以下の条件を全て満たす形式で侵害情報の送信防止措置の申出を受ける必要がある

1. 送信防止措置を要請するものが特定電気通信による情報の流通によって自己の権利を侵害されたとするものであること
2. 特定電気通信による情報の流通によって自己の権利を侵害されたとする情報であること
3. 侵害されたとする権利が特定されていること
4. 権利が侵害されたとする理由が述べられていること
5. 送信防止措置を希望することの意思表示があること

F.3.2　プロバイダ等による自主的送信防止措置の要否

送信防止措置の要請や違法情報が掲載されている旨の苦情を受けた場合，当該情報が他人の権利を侵害しているか否かは，プロバイダ等なりの判断とされる．しかし，当該情報が他人の権利を侵害していることが上記の判断基準に従い明らかである場合，申告者との関係は「他人の権利が侵害されていることを知ることができたと認めるに足りる相当の理由があるとき」に該当するため，自主的に送信防止措置を講じないと，損害賠償責任を負わされる可能性がある．またこの場合は，発信者からの損害賠償責任性急に応じるリスクはないといっていい場合である．

しかし，実際には，判断基準に照らしても，送信防止措置を講じても差し支えないかどうかの判断がつかない場合が多い．その場合は，照会手続きをとることができる．

F.3.3　照会手続きの手順

プロバイダ等において更新防止措置を講じても差し支えないかどうかの判断がつかない場合，照会手続きを利用することができる利用することができる．

- 申立者の確認照会手続きにおいては，自己の権利を侵害されたとするものまたは，その代理人が要請しなければならないので，以下の手順で本人確認をする．
  - 書面
    三ヶ月以内の印鑑登録証明書を添付の上，実印で押印したもの

- 電子メール
  公的な電子署名所により本人が発信したメールであることが証明できる電子署名が付いていること
- 代理人
  上記の他に，代理人への委任状を添付してもらう

- 侵害情報等の特定照会手続きを開始するには，申立者本人またはその代理人から侵害情報等の通知を受けることが必要があり，通知を受けたプロバイダ等はこれらの侵害情報等を発信者に伝え，送信防止措置を講じるかどうかを照会する必要がある．

  このため，発信者が送信防止措置を講じることに同意するか否かを判断するに足りる侵害情報等が特定できない場合，通報者に不明瞭な点等を書式を修正して再提出してもらう必要がある．また，発信者に連絡する際には次の情報はそのまま知らせることが望ましい．

  - 自己の権利を侵害されたとする情報
  - 侵害されたとする権利
  - 権利が侵害されたとする理由
  - 送信防止措置を希望することの意思表示

  しかし，申立者の氏名等は，申立者が発信者との関係で氏名等を伏せることに合理的な理由がある場合があることから原則として非開示．

- 照会可能な場合プロバイダ等は発信者に対し，送信防止措置を講じるよう要請があったこと及び申立者から提供された侵害情報等を通知し，送信防止措置を講じることに同意するか否かを照会することができる．

- 照会ができない場合照会は法令上の義務ではないので，発信者と連絡することができない場合照会手続きを進める必要はない．この場合は，照会せずに即時に送信防止措置を講じても差し支えない場合に該当していれば，プロバイダ等の判断で実行可能．一方，即時の判断が不可能な場合，発信者からの訴訟リスクを考慮して静観するか，申立者からの訴訟リスクを考慮して送信防止措置を講じるかのいずれかの対応となる．

- 照会手続き前述の条件が揃った場合，送信防止措置を遅延なくおこなうことが望ましいとされるが，自主的な解決方法模索のため等に時間がかかったりして遅延が発生しても照会手続き遅延の責任は負わないと考えられる．

  照会手続きは，基本的に当該照会が発信者に到達した日の翌日から起算して七日以内に発信者からの反論があるかどうかを確認する．

- 照会に対し発信者から送信防止措置を講じることに同意しない旨の回答があったとき照会をおこなうということは,「他人の権利が侵害されていることを知ることができたと認めるに足りる相当の理由」がない場合であるから，発信者から反論がなされた場合，その反論が明らかに理由のないものである場合を除き，損害賠償責任を免れるものと考えられる．また，発信者との関係において,「相当の理由」がないと判断して照会をおこなったのに，反論が明らかに理由のな

いものである場合を除き，送信防止措置を講じれば作為責任を問われる恐れがある．

F.3.4　法務省人権擁護機関からの情報削除依頼への対応

- 受付法務省人権擁護機関からの情報削除依頼に対応するためには，以下の条件が必要である．基本的に依頼は書面でおこなわれる必要がある．
  - 法務省人権擁護機関からの依頼であること
  - 侵害情報等の特定
  - 侵害されたとする権利の特定及び権利侵害の理由が明白であること
- 送信防止措置の要因の検討以下のいずれかに該当する場合，法務省人権擁護機関からの削除依頼として対応すべきかどうか弁護士等の専門家に相談の上対応することが望ましい．
  - 法務省人権擁護機関からの依頼であることが確認できないとき
  - 法務省人権擁護機関から示された場所に侵害情報がないとき
  - 侵害されたとする権利が特定されてないとき
  - 本ガイドライン等の判断基準に照らして，他人の権利を侵害したとする情報の違法性が明白でないとき
  - 侵害情報を削除することにより他の無関係の情報を大量に削除してしまうこととなる場合等,「必要な限度」を超える措置をなってしまうとき
- 送信防止措置を講じないこととした場合上記に上げる事由に一つでも該当する場合で，法務省人権擁護機関からの削除依頼に応じることのできない理由があると認める場合，法務省人権擁護機関に追加で説明を求めることができる．また，任意ではあるが，削除依頼が本ガイドラインの基準を満たしてない場合には，その旨を通知することが望ましい．

F.3.5　送信防止措置以外の対応

プロバイダ等は，申立者から申告があった情報について自ら送信防止措置を講じる必要まではないと判断した場合であっても，以下のような措置を講じることが望ましい．

- 照会手続き等から発信者と申立者との直接交渉による紛争解決を促す
- 特定電気通信役務提供者が複数存在する場合は，管理責任の大きいほうに対応を求める

付 録G　電子タグに関するプライバシー保護ガイドライン

このガイドラインは，経済産業省商務情報制作局長及び商務流通審議官の諮問研究会である「商品トレーサビリティの向上に関する研究会」がパブリックコメントを求めた上で，その結果を踏まえて取りまとめた物である．

当研究会では，問題が発生してからでは対応が後手に回りかねないことから，現段階においてプライバシー保護のための具体的なガイドラインを制定し，関係事業者団体に周知していくことが重要と考え，本ガイドラインを制定し，公表することにした．

以下に概要を記述する．

G.1　電子タグに関する消費者プライバシー保護の必要性

個人情報の保護の問題については，電子タグを用いる場合においても「個人情報保護法」が提供されるのだが，電子タグを用いた収集されるデータの中には,「個人情報保護法」で定義されない情報もある．しかし，個人情報を取り扱わない場合にもプライバシー保護の問題が生じる場合があるのである．

また，電子タグ固有の特性は，未だ十分認識される状況にはなっていないので，消費者の気が付かないうちに消費者が望まない形で情報を読み取られる恐れが想定される．そのような状況に至る前に，電子タグ固有の特性から生じるプライバシ問題に向き合い，これにより電子タグが円滑に社会に受け入れられるようにすることが必要である．

我が国においては，ルールを定める際，およそ全ての詳細なこと項についてまで同意が得られないとルールを定めない場合が多いが，このような対応は後手に回り易いと云う問題点がある．従って，当研究会としては，電子タグが本格的に普及する前の現段階においても，個人のプライバシを保護するために以下のようなガイドラインを策定した．

G.1.1　目的

電子タグが持つ有用性に留意しつつ，消費者の利益を保護し，電子タグが円滑に社会に受け入れられるようにするため，電子タグに関する消費者のプライバシ保護に関し業種横断的に共通な基本的考え方を明らかにする

G.1.2　対象範囲

消費者に物品が渡されたあとも当該物品に電子タグを装着しておく場合

G.1.3　電子タグ装着に関する表示等

当該物品に電子タグが装着されている事実，装着箇所，その性質及び当該電子タグに記録されている情報の内容をあらかじめ説明もしくは掲示する（この際，きちんと消費者が認識できるよう努めること）．または，消費者がきちんと認識できるよう包装上等に表示をおこなう必要がある．

G.1.4　消費者の最終的な選択権の留保

消費者の選択により，当該電子タグの読み取りができないようにすることを容易にできるよう，その手法についてあらかじめ説明もしくは掲示，包装上に表示する必要がある．

G.1.5　社会的利益等に関する情報提供

電子タグの読み取りを出来ないようにした場合，それによって失われる情報がある場合，当該情報について表示，その他の方法で消費者に提供するする必要がある．例えば，

- 商品のリサイクルに必要な情報が失われることによる環境保全上の問題
- 自動車の修理履歴の情報が失われることによる安全への影響　等

G.1.6　タグ情報と個人情報データベースとの連携

個人情報データベースとの連携をおこなう場合は，当該情報は個人情報保護法上の個人情報としての扱いを受ける．

G.1.7　説明・情報提供

事業者，事業者団体及び政府機関等の関係機関は，消費者の電子タグに対する理解を助けることに努める必要がある．

G.1.8　事業者の行動

事業者は，本ガイドラインの基本的考え方に沿った上で，それぞれの実態に応じた消費者との関係を踏まえ，適切な対応をとることが望まれる．

G.1.9　ガイドラインの見直し

プライバシ保護についての考え方は，社会情勢の変化，消費者の認識の変化，技術の進歩等に応じて変わり得る物であり，本ガイドラインは，それら諸環境の変化を踏まえて見直しを図るものとする．

以上

参考文献

[1] Marc Langheinrich
Privacy by Design -Principles of Privacy-Aware Ubiquitous Systems-
In *proceedings of the third conference on Ubiquitous Computing (Ubicomp'01)*, September, 2001

[2] Marc Langheinrich
A Privacy Awareness System for Ubiquitous Computing Environments
In *proceedings of the third conference on Ubiquitous Computing (Ubicomp'02)*, September, 2002

[3] 山邉 哲生, 藤波 香織, 正寺 朋子, 中村 暢芳, 中島 達夫（早稲田大）
PENATES:コンテクストアウェアな環境下でのプライバシ制御のためのアーキテクチャ
In *proceedings of 16th Computer System Symposium (ComSys '04)* , November, 2004

[4] 安心して個人情報を取り扱うためには
財団法人インターネット協会
２００４年４月

[5] 明治学院大学社会学部　宮田加久子
東京大学大学院人文社会研究科　池田謙一
インターネットでの「評判」（reputation）と広告の実証的研究
平成１２年度吉田秀雄記念事業財団助成研究集

[6] トラストマークについて
TRUSTe-OnlinePrivacyResourceBook-

[7] 弁護士：牧野次郎
プライバシーとは何かープライバシー保護と個人情報保護の違いに関する考察ー
http://www.asahi-net.or.jp/ VR5J-MKN/point/privacy/

[8] 東京工業大学奥村研究室
ネット上の日記サイトからの情報収集
http://oku-gw.pi.titech.ac.jp/blogwatcher/

[9] 財団法人ニューメディア開発協会
各国のプライバシ保護について
http://www.nmda.or.jp/enc/privacy/privacy-now5.html
2000 年 11 月版

[10] Global Business Dialogue on Electronic Commerce 2001 提言書
http://www.gbde.org/recommendations.html
Tokyo Conference 2001

[11] Global Business Dialogue on Electronic Commerce 2002 提言書
http://www.gbde.org/recommendations.html
Brussels Conference 2002

[12] Global Business Dialogue on Electronic Commerce 2003 提言書
http://www.gbde.org/recommendations.html
New York Conference 2003

[13] 2003 年度 JNSA セキュリティポリシ WG 成果物
-脅威，脆弱性および残存リスク対応表について-
2004 年 4 月：セキュリティポリシ WG

[14] 山崎　哲
日本 IBM 株式会社：エグゼクティブコンサルタント
ネットワーク社会におけるセキュリティアーキテクチャの活用

[15] U.S. Copyright Office
The Digital Millennium Copyright Act of 1998
-U.S Copyright Office Summary- December 1998

[16] 原案作成団体：財団法人日本規格協会
個人情報保護に関するコンプライアンス・プログラムの要求事項 (JIS Q 15001)
平成１１年４月２日：日本工業規格

[17] NPO 日本ネットワークセキュリティ協会脅威，脆弱性及び残存リスク対応表について
2003 年度 JNSA セキュリティポリシ WG 成果物

[18] RFID のプライバシー懸念を緩和する新セキュリティ技術
CNET Japan 2003/08/28

[19] RFID タグ，今後は囚人の監視にー米オハイオ州ー
CNET Japan 2004/08/03

[20] ようこそ RFID ランドへーテーマパークでも採用広がるー
CNET Japan 2004/09/15

[21] 経済産業省
「電子タグに関するプライバシー保護ガイドライン」
平成１６年３月１６日

[22] 安田雪　著
ネットワーク分析-何が行為を決定するか-
新曜社

[23] 名古屋大学教授　加賀山　茂
消費者の自己責任を考える
http://www.nomolog.nagoya-u.ac.jp/
kagayama/consumer/resume/jikosekinin.html

[24] バイロンリーブス・クリフォードナス　著
人はなぜコンピュータを人間として扱うか
翔泳社

[25] Susannah Fox, Director of Research
Trust and privacy online :
Why Americans want to rewrite the rules
The Pew Internet and American Life Project 2000

[26] Princeton Survey Research Associates
A Matter of Trust :
What Users Want From Web Sites
Consumer WebWatch Transparency Survey 2002

[27] 山岸俊男
安心社会から信頼社会へ
http://www.asahi-net.or.jp/ eh6k-ymgs/book/shakaishiso/
tosho-y/anshin-shinrai.htm

[28] 高谷邦彦
http://www.wakhok.ac.jp/ saitoh/literacy-9
2002 年